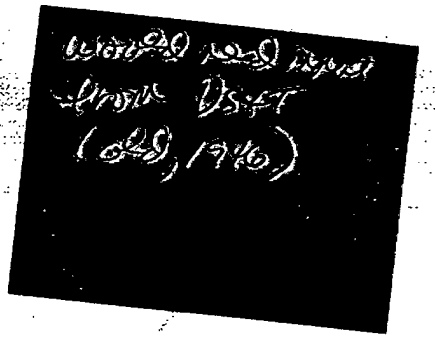
all from DOC
FBI & FF cons 1st
go to Amn for Release



Document

1305109

STR
of
NDRC

Div 1
Vol 3

SPEECH SCRAMBLING

OSRD

# SUMMARY TECHNICAL REPORT
# OF THE
# NATIONAL DEFENSE RESEARCH COMMITTEE



SECRET

Would need input from DS&T (old, 1946).

Manuscript and illustrations for this volume were prepared for publication by the Summary Reports Group of the Columbia University Division of War Research under contract OEMsr-1131 with the Office of Scientific Research and Development. This volume was printed and bound by the Columbia University Press.

Distribution of the Summary Technical Report of NDRC has been made by the War and Navy Departments. Inquiries concerning the availability and distribution of the Summary Technical Report volumes and microfilmed and other reference material should be addressed to the War Department Library, Room 1A–522, The Pentagon, Washington 25, D. C., or to the Office of Naval Research, Navy Department, Attention: Reports and Documents Section, Washington 25, D. C.

Copy No.

**149**

This volume, like the seventy others of the Summary Technical Report of NDRC, has been written, edited, and printed under great pressure. Inevitably there are errors which have slipped past Division readers and proofreaders. There may be errors of fact not known at time of printing. The author has not been able to follow through his writing to the final page proof.

Please report errors to:

JOINT RESEARCH AND DEVELOPMENT BOARD
PROGRAMS DIVISION (STR ERRATA)
WASHINGTON 25, D. C.

A master errata sheet will be compiled from these reports and sent to recipients of the volume. Your help will make this book more useful to other readers and will be of great value in preparing any revisions.

SECRET

SUMMARY TECHNICAL REPORT OF DIVISION 13, NDRC

VOLUME 3

# SPEECH AND FACSIMILE SCRAMBLING AND DECODING

OFFICE OF SCIENTIFIC RESEARCH AND DEVELOPMENT
VANNEVAR BUSH, DIRECTOR

NATIONAL DEFENSE RESEARCH COMMITTEE
JAMES B. CONANT, CHAIRMAN

DIVISION 13
HARADEN PRATT, CHIEF

WASHINGTON, D. C., 1946

~~SECRET~~



Declassified and Approved For Release 2013/12/11 : CIA-RDP10T02279R000100180001-2

# NATIONAL DEFENSE RESEARCH COMMITTEE

James B. Conant, *Chairman*

Richard C. Tolman, *Vice Chairman*

| | |
|---|---|
| Roger Adams | Army Representative[1] |
| Frank B. Jewett | Navy Representative[2] |
| Karl T. Compton | Commissioner of Patents[3] |

Irvin Stewart, *Executive Secretary*

[1]*Army representatives in order of service:*

Maj. Gen. G. V. Strong
Maj. Gen. R. C. Moore
Maj. Gen. C. C. Williams
Brig. Gen. W. A. Wood, Jr.
Col. L. A. Denson
Col. P. R. Faymonville
Brig. Gen. E. A. Regnier
Col. M. M. Irvine
Col. E. A. Routheau

[2]*Navy representatives in order of service:*

Rear Adm. H. G. Bowen
Capt. Lybrand P. Smith
Rear Adm. J. A. Furer
Rear Adm. A. H. Van Keuren
Commodore H. A. Schade

[3]*Commissioners of Patents in order of service:*

Conway P. Coe
Casper W. Ooms

## *NOTES ON THE ORGANIZATION OF NDRC*

The duties of the National Defense Research Committee were (1) to recommend to the Director of OSRD suitable projects and research programs on the instrumentalities of warfare, together with contract facilities for carrying out these projects and programs, and (2) to administer the technical and scientific work of the contracts. More specifically, NDRC functioned by initiating research projects on requests from the Army or the Navy, or on requests from an allied government transmitted through the Liaison Office of OSRD, or on its own considered initiative as a result of the experience of its members. Proposals prepared by the Division, Panel, or Committee for research contracts for performance of the work involved in such projects were first reviewed by NDRC, and if approved, recommended to the Director of OSRD. Upon approval of a proposal by the Director, a contract permitting maximum flexibility of scientific effort was arranged. The business aspects of the contract, including such matters as materials, clearances, vouchers, patents, priorities, legal matters, and administration of patent matters were handled by the Executive Secretary of OSRD.

Originally NDRC administered its work through five divisions, each headed by one of the NDRC members. These were:

Division A—Armor and Ordnance
Division B—Bombs, Fuels, Gases, & Chemical Problems
Division C—Communications and Transportation
Division D—Detection, Controls, and Instruments
Division E—Patents and Inventions

In a reorganization in the fall of 1942, twenty-three administrative divisions, panels, or committees were created, each with a chief selected on the basis of his outstanding work in the particular field. The NDRC members then became a reviewing and advisory group to the Director of OSRD. The final organization was as follows:

Division 1—Ballistic Research
Division 2—Effects of Impact and Explosion
Division 3—Rocket Ordnance
Division 4—Ordnance Accessories
Division 5—New Missiles
Division 6—Sub-Surface Warfare
Division 7—Fire Control
Division 8—Explosives
Division 9—Chemistry
Division 10—Absorbents and Aerosols
Division 11—Chemical Engineering
Division 12—Transportation
Division 13—Electrical Communication
Division 14—Radar
Division 15—Radio Coordination
Division 16—Optics and Camouflage
Division 17—Physics
Division 18—War Metallurgy
Division 19—Miscellaneous
Applied Mathematics Panel
Applied Psychology Panel
Committee on Propagation
Tropical Deterioration Administrative Committee

# NDRC FOREWORD

As EVENTS of the years preceding 1940 revealed more and more clearly the seriousness of the world situation, many scientists in this country came to realize the need of organizing scientific research for service in a national emergency. Recommendations which they made to the White House were given careful and sympathetic attention, and as a result the National Defense Research Committee [NDRC] was formed by Executive Order of the President in the summer of 1940. The members of NDRC, appointed by the President, were instructed to supplement the work of the Army and the Navy in the development of the instrumentalities of war. A year later, upon the establishment of the Office of Scientific Research and Development [OSRD], NDRC became one of its units.

The Summary Technical Report of NDRC is a conscientious effort on the part of NDRC to summarize and evaluate its work and to present it in a useful and permanent form. It comprises some seventy volumes broken into groups corresponding to the NDRC Divisions, Panels, and Committees.

The Summary Technical Report of each Division, Panel, or Committee is an integral survey of the work of that group. The first volume of each group's report contains a summary of the report, stating the problems presented and the philosophy of attacking them, and summarizing the results of the research, development, and training activities undertaken. Some volumes may be "state of the art" treatises covering subjects to which various research groups have contributed information. Others may contain descriptions of devices developed in the laboratories. A master index of all these divisional, panel, and committee reports which together constitute the Summary Technical Report of NDRC is contained in a separate volume, which also includes the index of a microfilm record of pertinent technical laboratory reports and reference material.

Some of the NDRC-sponsored researches which had been declassified by the end of 1945 were of sufficient popular interest that it was found desirable to report them in the form of monographs, such as the series on radar by Division 14 and the monograph on sampling inspection by the Applied Mathematics Panel. Since the material treated in them is not duplicated in the Summary Technical Report of NDRC, the monographs are an important part of the story of these aspects of NDRC research.

In contrast to the information on radar, which is of widespread interest and much of which is released to the public, the research on subsurface warfare is largely classified and is of general interest to a more restricted group. As a consequence, the report of Division 6 is found almost entirely in its Summary Technical Report, which runs to over twenty volumes. The extent of the work of a Division cannot therefore be judged solely by the number of volumes devoted to it in the Summary Technical Report of NDRC; account must be taken of the monographs and available reports published elsewhere.

Of all the NDRC Divisions, few were larger or charged with more diverse responsibilities than Division 13. Under the urgent pressure of wartime requirements, the staff of the Division developed navigation and communications devices and systems which not only contributed to the successful Allied war effort, but which will continue to be of value in time of peace in the fields of transportation and communications. The work of the Division, under the direction first of C. B. Jolliffe and later of Haraden Pratt, furnishes a foundation for what promises to be even more radical developments than those of the war—for one example, direction finders which will operate at all elevations and azimuth angles, in other words, hemispherically.

The Summary Technical Report of Division 13 was prepared under the direction of the Division Chief and authorized by him for publication. The report presents the methods and results of the widely varied research and development program, and, in the case of work with speech scrambling and decoding, it presents for the first time a comprehensive review of the state of the art. The report is also a notable record of the skill and integrity of the scientists and engineers, who, with the cooperation of the Army and Navy and Division contractors, contributed brilliantly to the defense of the nation. To all of these we express our sincere appreciation.

VANNEVAR BUSH, Director
*Office of Scientific Research and Development*

J. B. CONANT, Chairman
*National Defense Research Committee*

# FOREWORD

EARLY IN OCTOBER 1940 a subcommittee on speech secrecy was set up in the Communications Division of the National Defense Research Committee [NDRC], later known as Division 13 of NDRC. This group was to consider both the scrambling and unscrambling of telephone signals. It was soon recognized that the decoding problem was of primary importance both as a means of evaluating privacy systems for possible use by the Services and for decoding possible enemy signals. Thus the work under Division 13 on speech privacy took on two aspects, that of providing "secure" means of voice, code, and picture communication, and that of decoding transmissions for the dual purpose of learning how useful were our own secrecy systems and for learning what the enemy might be saying in his scrambled messages.

Numerous projects were carried forward under the guidance of the Division, some of them with the object of developing scrambling or secrecy methods, others dealing entirely with code cracking methods. In this way the work accomplished on methods of secrecy could be tested at every phase by the decoding groups which were also busy on other aspects of the decoding problem. The summaries to follow will disclose the objects and accomplishments of the individual projects.

Work on speech secrecy problems went on in the Division from 1940 quite to the end of the war, the final report on Project 13-106 being issued on August 18, 1945. Thus, this volume summarizes the results of about five years' experience in developing secrecy systems and in diagnosing, decoding, and evaluating these and other systems submitted for study by the Army, the Navy, and NDRC.

All these studies are reported in detail in the preliminary and final reports on the projects and are only summarized here. The sum of these reports, therefore, provides a record of accumulated experience, much of which has never been reported in any other way. In toto, the reports make available information both positive and negative which would have to be accumulated by another group if they were to embark on a similar project.

The immediate pressure behind these studies was caused, of course, by the war. The work summarized in this volume, therefore, should serve as a guide to the individual reports and should aid a newcomer to the field in becoming properly oriented to the state of the art so far as the NDRC project reports are concerned. Other work, carried out in other government groups, is not believed to duplicate this material.

In passing, it is worth noting that, in contrast to a rather extensive literature on code and cipher systems, and on cryptanalysis and cryptography, which apply to telegraphic types of communication, very little has been written on speech privacy systems or decoding methods applying to them. Two moderately comprehensive articles have been published. One appeared in the *Post Office Engineers Journal*, October 1933; the other, in the *Brown Boveri Review* for December 1941. The latter report is reproduced and discussed in Preliminary Report No. 5, Project C-43. It covers a number of basic types of scrambling systems and, in addition, discloses one that was new at the time. This is a modification of the "time division scrambling" or TDS system, and several of the Division 13 projects were concerned with this useful privacy method.

Without any doubt, one of the major accomplishments of the Division's work and certainly the high point in its efforts within the subject matter of this volume was the development of the sound spectrograph by Mr. R. K. Potter and his co-workers at the Bell Telephone Laboratories. The efficacy of this instrument in analyzing scrambled speech will be revealed in the chapters to follow.

HARADEN PRATT
Chief, Division 13

# PREFACE

IN SUMMARIZING the several hundred reports of contractors on the hundred-odd research projects sponsored by Division 13 of the National Defense Research Committee, the editor has had to settle in his own mind how much or how little of each project report should be included; in other words, how far the boiling-down process should go.

The editor has an abhorrence for seeing good scientific or technical material go unpublished. Only by publication can the facts or methods developed by a few researchers become available for all researchers. On this basis, substantially all of Division 13's program should be included in the volumes, of which this is one, summarizing the work of the Division. On the other hand, time moves forward inexorably so that it is quite likely that, by the day of publication, much of the data would already be out of date. Furthermore, time and human energy are always scarce. On these bases, all that might be required would be a paragraph or two summarizing the aims of the project and its accomplishments.

A middle course was steered, a course between the easiest solution of publishing practically all of each report and the more difficult job of really digesting the project purpose and results. The editor, however, deliberately chose to publish too much rather than too little. In most cases it will be unnecessary for the reader to search out the original source material unless he wishes to dig deep into the subject. In those cases where fundamental information was assembled and printed in the project report, that is, information on which future research might be based, the summaries have been permitted to take as much space as required.

The plan followed in this volume is briefly as follows: After a comprehensive description of the several scrambling methods, brief summaries are given of the work carried out in the several projects dealing with scrambling. Then follows a comprehensive description of decoding or cracking methods employed, after which are summaries of the projects dealing mainly with decoding or code cracking. In other words, most of the space is devoted to basic material and the least space to details of the actual work carried out. Thus this volume might be considered as a basic text on speech scrambling and descrambling.

The material is not arranged chronologically with respect to the order of the work in the Division but, rather, in an arrangement which appeared to the editor as giving the reader the easiest and quickest approach to the whole subject of speech privacy and code cracking. Thus, parts of the individual project reports will be found in several places in this volume.

KEITH HENNEY
Editor

# CONTENTS

# Chapter 1

# SPEECH SCRAMBLING METHODS

A WIDE VARIETY of speech scrambling methods will be examined in this chapter, taken from Part I of the final report[1] of Project C-43, in order to become familiar with the devices which might be used alone or in combination to make up speech privacy systems. Some of these systems are in commercial or military use, others exist only on paper, mostly in the form of patents or patent applications. It is not intended to include all the variations of all the different methods but rather to cover basic scrambling methods, with their most important variations, in which the original speech is transmitted with its parts modified, displaced, or interchanged.

The two main dimensions of speech which are operated upon to make it unintelligible are the frequency dimension and the time dimension. Scrambling systems usually depend on rearranging the components of speech in either or both of these dimensions. In general it may be said that those that operate on the frequency dimension alone are capable of the best quality in the reproduced speech. A complete list of the systems covered in the discussion is given in Table 1 of Chapter 4, together with other data concerning them.

## 1.1 SYSTEMS INVOLVING SINGLE MODULATION

A basic device in privacy systems is the modulator. One form of modulator, shown in Figure 1A, consists of four copper oxide varistor units between two balanced coils. The carrier frequency is fed into the midpoints of the coils as shown. In some cases the coils can be omitted as shown in Figure 1B.

Figure 2 shows the method of producing simple inversion. In this and in succeeding illustrations the numerical values are not necessarily the best values for practical operation, but they serve to illustrate the manner in which the device operates.

In the system shown in Figure 2 the speech band is limited to 3 kc by a low-pass filter. It is then modulated with a frequency of 3 kc. This produces an upper and a lower sideband of which only the latter is passed by the output filter. The system is called inversion, because the high frequencies in the original speech appear as low frequencies in the output and the low frequencies in the original speech appear as high frequencies. At the receiving end the inverted signal, in passing through an identical system in the same direction, is reinverted back to normal speech.

A very commonly proposed variation of this system involves using a variable frequency instead of the steady 3-kc carrier. We might vary the frequency continuously or in discrete steps. It should be noted, however, that the cutoff of the low-pass output filter is fixed, which limits the variation permissible in the carrier frequency. A wide variation would either permit too much of the upper sideband to get through or would cut off some of the lower sideband.

If the modulator in Figure 2 is of the type shown in Figure 1A, speech can be scrambled by introducing instead of the 3-kc carrier a square wave whose changes from positive to negative value are irregular in time. Each one of the reversals in the carrier wave causes a

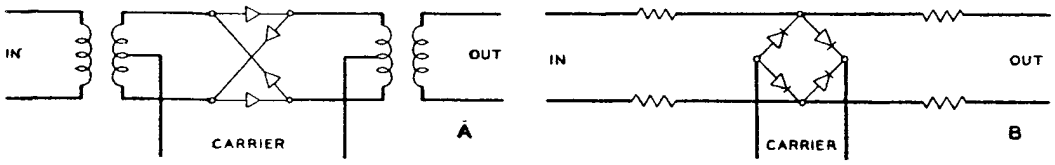



FIGURE 1. Use of copper oxide varistors as modulators. In A, balanced coils are necessary; in B, coils are not required.

reversal of phase in the speech wave. The pattern of these irregular reversals may be arranged so that the speech becomes unintelligible. At the receiving end a coding wave must be introduced which is exactly in step with the

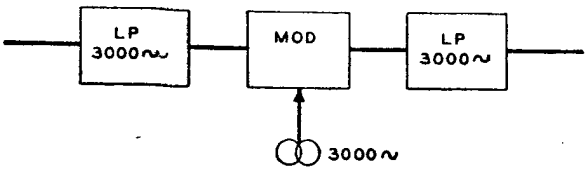



FIGURE 2. Simple inversion produced by single modulation.

one at the receiving end with proper allowance for any delay there may be in the transmitting channel.

A two-channel system using one modulator for each channel is shown in Figure 3. In this system the carrier fed into both modulators is the same in frequency but differs 90 degrees in phase. Two separate speech channels can be transmitted by this method without substantial mutual interference, but both sidebands as well as the carrier must be transmitted. At the receiving end the carrier must be split into two components with the proper phases. Each component will demodulate its own portion of the signal and thereby separate the two speech channels. One of the channels may consist of noise or spurious speech from a recording or the like, which tends to mask the real message if the signal is demodulated with an ordinary set. This scheme was originally proposed as a multiplex system, but an obvious variation is to divide a single speech band into two halves with filters and then transmit the two halves on carriers differing by 90 degrees in phase.

## 1.2 SYSTEMS INVOLVING DOUBLE MODULATION

Figure 4 shows a much more flexible system. Here the signal is modulated twice, with a band-pass filter between the two modulators. With this arrangement the carrier frequency fed into the second modulator can be varied in several ways. In the illustration two carrier frequencies are shown for the second modulator. If the 8-kc value is used the output consists of the speech band right side up but displaced from its normal position by 2 kc. If the 16-kc value is used the output consists of the 3-kc speech band inverted and displaced by 3 kc. We might use these two values alternately at short intervals, or we might have the carrier

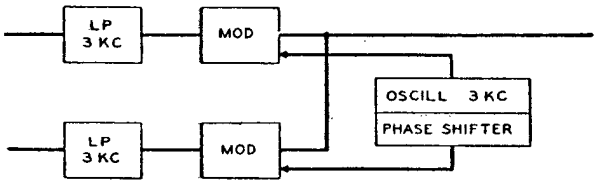



FIGURE 3. Split-phase multiplex used as two-channel system.

vary continuously back and forth, say between 13 and 16 kc. Another variation is to use a multiplicity of values, for example, 500 or 1,000 cycles apart, (not between 10 and 13 kc for this illustration) and switch between these values in a regular or irregular sequence. A

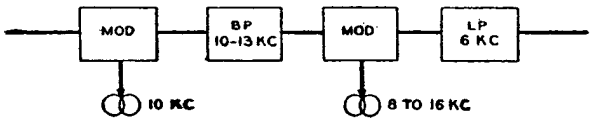



FIGURE 4. System in which signal is modulated twice, requiring wider frequency band than is usually provided by radio sets or telephone lines.

disadvantage of these systems is that the transmission channel needs to be wider than that usually afforded by radio sets or telephone lines. In all these systems, the speech is restored by passing through identical equipment in the opposite direction.

## 1.3 TRIPLE MODULATION—RE-ENTRANT BAND SHIFT

Going back to Figure 2, suppose the carrier frequency were made 4 instead of 3 kc, but the 3-kc input and output filters were retained. The output would then be an inverted sideband ranging from 1 to 3 kc; that portion of the sideband above 3 kc would be cut off by the output filter. Since, however, there is a 1-kc gap at the lower edge of the transmitted band, the portion which would be cut off by the filter might be modulated down and sent along with the rest of the signal in this lower part of the

spectrum. In other words the portion of the sideband which would otherwise disappear above the upper edge of the transmitted band might be made to reappear at the bottom.

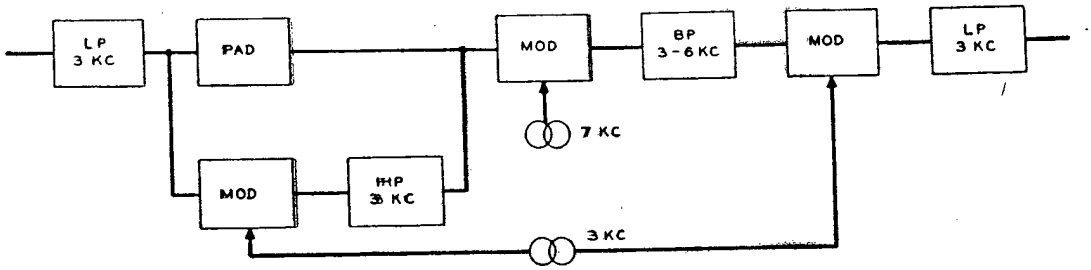



FIGURE 5. System involving re-entrant inversion.

Figure 5 shows a system of modulators and filters for accomplishing this kind of band shift. The first modulator is followed by a high-pass filter which selects the upper sideband from 3 to 6 kc. This is combined with some of the original signal which ranges from zero to 3 kc. The second modulator is fed with a carrier frequency of, for example, 7 kc which inverts the whole band. This is followed by a band-pass filter passing the range from 3 to 6 kc. A third modulator with its carrier frequency placed at the lower edge of the 3- to 6-kc input band moves the whole band, still inverted, down to the usual range of zero to 3 kc. The upper sideband of this modulation step is removed by the output low-pass filter. A variation of this arrangement is to allow the 7-kc carrier to vary in discrete steps according to some regular or irregular program or vary it continuously between the limits of 6 to 9 kc. This provides a variable band-shifting arrangement without using more than the normal 3-kc transmission channel.

## 1.4 BAND-SPLITTING SYSTEMS

A privacy system in wide commercial use, known as the split-band system, involves splitting up the whole speech band into a number of subbands and shifting these around out of their normal positions in the frequency spectrum. Figure 6 shows one manner in which this can be accomplished. The numerical values

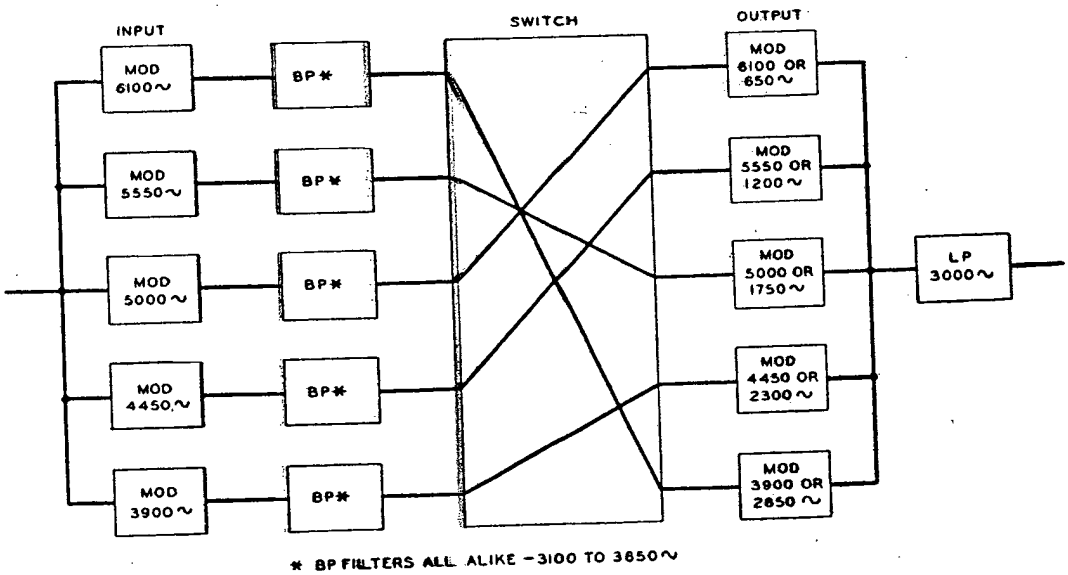



FIGURE 6. One form of split-band system in commercial use.

are chosen so that the band from 250 to 3,000 cycles is divided into five subbands each 550 cycles wide.

The speech band is fed to five modulators in parallel. The five band filters following the modulators are all alike, passing the band from 3,100 to 3,650 cycles. It will be seen that the uppermost modulator in Figure 6 with its carrier of 6.1 kc will invert the speech band and displace it by such an amount that the frequency band which originally occupied the space from 2,450 to 3,000 cycles will pass through the filter. In other words, this modulator in combination with its band filter selects the uppermost of the five subbands from the input signal. Similarly the lowest modulator in combination with its band filter selects the lowest subband from the input signal. The outputs of the band filters all occupy the same frequency range, but they all came originally from different frequency ranges. Similarly the output modulators are so designed that each one accepts the band from 3,100 to 3,650 cycles and shifts it to a particular band location in the output. The five leads going into the box labeled "switch" may, therefore, be cross-connected in any desired manner with the five output leads. The resulting output will always cover the complete range from 250 to 3,000 cycles and there will be no overlapping subbands.

An additional set of frequencies is indicated in the drawing for the second set of modulators. These frequencies will cause the output subbands to be inverted instead of right side up. One or all of these alternate frequencies may be used as desired.

The "switch" may be changed as often as desired. On an experimental basis the codes have been changed as often as 25 times per second without appreciable distortion in the quality of the received speech, showing that it is possible to shift bands as wide as 550 cycles at a rapid rate without generating appreciable distortion products.

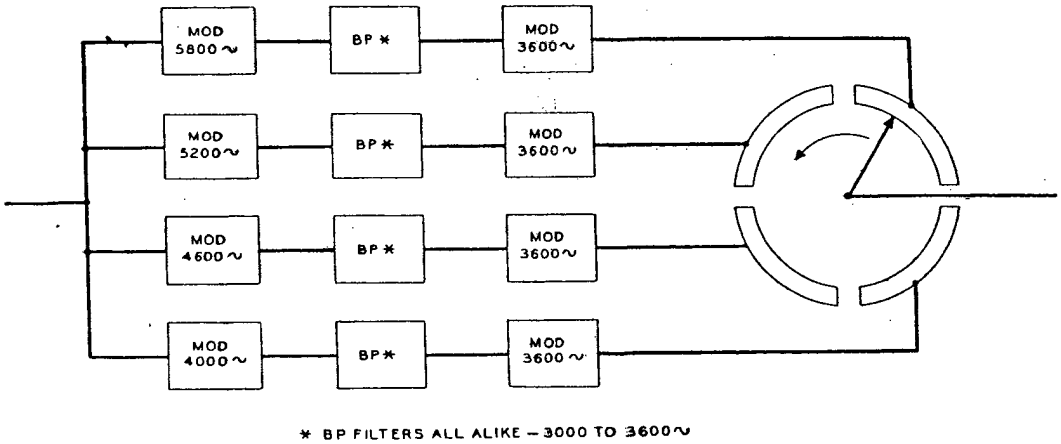



FIGURE 7. Time division multiplex in which $N$ separate signals are sent over line, each signal being transmitted only $1/N$th of time.

## 1.5 TIME DIVISION MULTIPLEX

Time division multiplex [TDM] is a system in which $N$ separate signals occupying the same frequency range are sent over a single line, each signal being transmitted only $1/N$th of the time. This might be illustrated by showing the $N$ signals connected to the $N$ segments of a commutator. A rapidly rotating brush picks up the $N$ signals one after the other. For acceptable quality, however, the brush must make at least as many rotations per second as the highest frequency in the transmitted signal. This means that a mechanical brush is out of the question and is used simply for illustration. This kind of switching, however, can be accomplished with electronic ring circuits.

Since we are interested here in privacy systems rather than multiplex systems, we will confine ourselves to the use of TDM for transmitting a single speech channel. This can be accomplished by dividing the speech band into a number of subbands all occupying the same frequency range, and connecting these to the segments of our hypothetical commutator. Referring to Figure 7, which is similar to Figure 6, this can be accomplished by feeding all the output modulators with the same carrier, and connecting each modulator to a commutator segment. In this illustration, there are four 600-cycle subbands, covering the range from 400 to 2,800 cycles. It has been shown mathematically that the output of this system consists of sidebands around a frequency corresponding to the rotation of the brush and also sidebands around frequencies corresponding to odd harmonics of the rotation frequency. Each sideband, however, contains components from each of the subbands. It has also been shown that the total channel width required for good transmission need be no greater than that of the original signal.

To increase the privacy of this system one of the subbands may be replaced by a band of noise. This can be filtered out at the receiving end. Obviously this system requires a high degree of synchronism between the two ends.

## 1.6 SYSTEMS USING TAPE RECORDING

Leaving the frequency substitution systems for the time being, we will introduce a device which permits operating on the time scale. The most versatile device for this purpose is the magnetic tape recording and reproducing system. This takes the form of a tape of magnetic alloy a few mils thick either run as a loop over pulleys or attached firmly to the perimeter of a disk. The recording is done by means of small electromagnetic pole-pieces. The signal is picked up by similar pole-pieces which may be placed at a distance from the recording pole-piece depending on the amount of delay desired. The outstanding advantage of the magnetic tape system for this type of application is that the signal may be erased and the recording medium be used over and over again. The quality of this type of transmission can be made very good with proper design.

Figure 8 shows a rather simple privacy system using magnetic tape. The input signal is passed through a 3-way pad, whereby it is impressed on a band filter, and also recorded

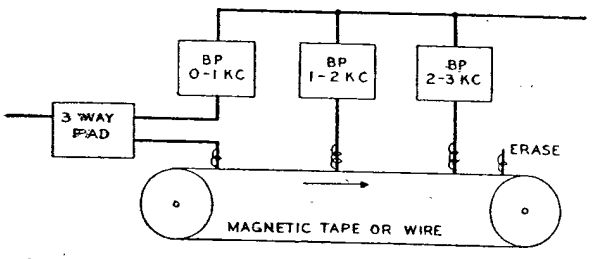



FIGURE 8. Variable subband delay system using magnetic tape.

on the magnetic tape. It is picked up by equally spaced pole-pieces each associated with a different band filter. With the arrangement shown in Figure 8 the band from 0 to 1 kc is transmitted without delay. The band from 1 to 2 kc is transmitted with 100 msec (0.1 sec) delay and the band from 2 to 3 kc is delayed 200 msec. At the receiving end the scrambled signal is passed through an identical system in the same way except that the two extreme band filters are interchanged. In this way the band which received no delay in transmission is given maximum delay in the receiving machine, and the band which received maximum delay in transmission is given zero delay in the receiver. In this way all the bands are delayed the same amount and the speech is restored to normal.

This system alone does not provide any high degree of privacy, but it can be combined with other systems, as we shall see.

## 1.7 TIME DIVISION SCRAMBLING

An important class of scrambles involving magnetic tape is known as time division scrambling [TDS]. A simplified diagram of this system is shown in Figure 9. There are a recording pole-piece and a number of pickup pole-pieces. There is also a commutator driven in synchronism with the tape. The length (in time) of each segment of the commutator is,

in general, equal to the delay between successive pickup pole-pieces. However, the number of segments need not be the same as the number of pole-pieces. A switch is provided whereby any segment may be connected to any pole-piece.

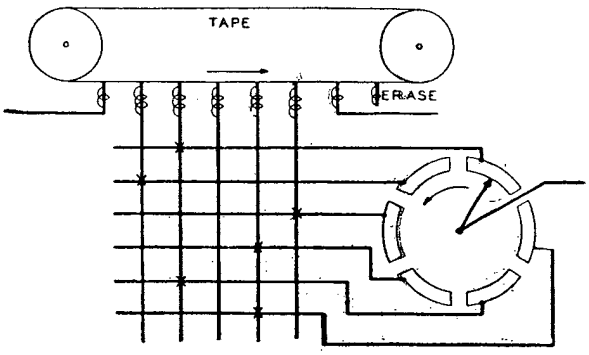



FIGURE 9. One form of time division scrambling [TDS].

With this system the speech is cut up into time elements corresponding in length to the spacing of the pole-pieces. These time elements are transmitted in a scrambled order. For instance, six successive time elements which we might label 1, 2, 3, 4, 5, 6 might be transmitted in the order 2, 4, 1, 3, 6, 5. The possibilities of TDS coding are far too complex to cover here. The general requirements for all TDS systems may be stated as follows: (1) Each element of the original speech must be transmitted once and only once. (2) The sum of the delay in the transmitting machine plus the delay in the receiving machine must be equal for all elements. With these two requirements fulfilled it is obvious that the speech comes out of the receiving machine in its normal order. It is delayed, however, by an amount equal to the sum of the transmitting and receiving delay.

At the receiving end there are several ways of handling the scrambled signal. (1) The pick-up pole-pieces can be used as recording pole-pieces and the signal picked up by an additional pole-piece shown at the right in Figure 9. With this arrangement the connections between the commutator and the pole-pieces are the same in the transmitting and receiving machines. (2) The signal can be recorded with the same pole-piece used in the transmitting machine and the connections between the pole-pieces and the segments rearranged for receiving by a push-to-talk relay. (3) The codes can be restricted to a particular class called self-converse codes. These have the property of being self-decoding, that is, the same code which scrambles the speech in the transmitter restores it in the receiver.

## 1.8 INTERLACE

An important variation of this system is called "interlace." In this system the number of segments on the commutator is doubled. The odd segments are connected to the pole-pieces according to one code and the even segments are connected according to a completely independent code. The reason for this device is to increase the difficulty encountered by the enemy in trying one code after the other to find the right one, particularly if the total number of codes available is small. With the interlace system the total number of combinations possible is equal to the square of the number of codes.

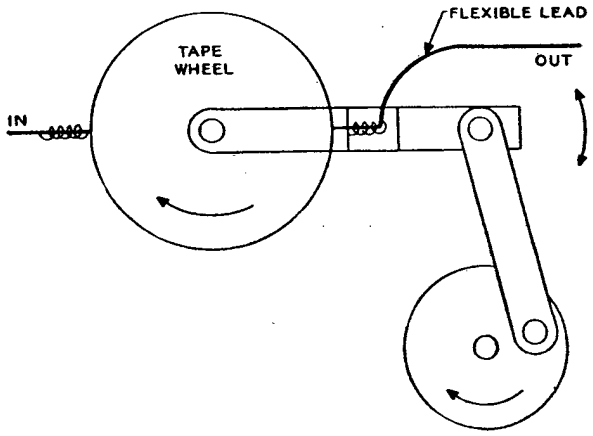



FIGURE 10. Speed wobble in which speech time scale is alternately compressed and expanded.

The rotating commutator shown in Figure 9 results in a repeated code, that is, each rotation produces the same scramble. It is possible to substitute for the commutator and switch arrangement, shown in Figure 9, a more complex arrangement whereby the speech is scrambled in a never repeating manner. There

are several ways of accomplishing this. Perhaps the simplest way to represent it is as a punched tape which permits the pole-pieces to be connected to the output, one at a time, in any desired order permissible under the restrictions outlined above.

Another way of utilizing magnetic tape to scramble speech is shown in Figure 10. Here the pickup pole-piece is oscillated back and forth along the tape mechanically. With this arrangement, or other variations equivalent to speech changes, the speech time scale is alternately compressed and expanded. The frequency scale is correspondingly expanded and compressed, respectively.

With the arrangement shown in Figure 11, speech is broken up into time segments each

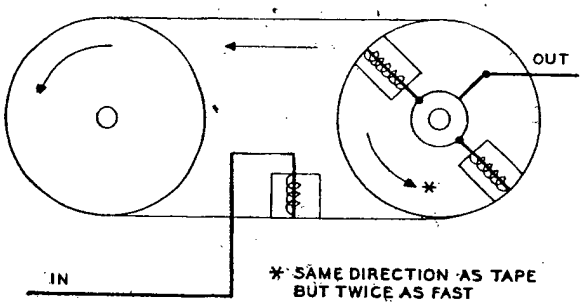



FIGURE 11. Time inversion in which speech is broken up into time segments, each of which is transmitted backwards.

of which is transmitted backwards. The motion of the pickup pole-pieces is twice as great as the motion of the tape and is in the same direction. Therefore, the relative motion of the tape and the pole-pieces is the reverse of that used in recording. This is the same as running the tape backwards for reproduction.

## 1.9 COMBINATIONS OF TIME AND FREQUENCY SCRAMBLING

Obviously the two kinds of systems described in the previous sections can be used together. For instance, some of the time elements of a TDS system might be inverted according to a regular or irregular program. The next more complex step is to combine the band-splitting system of Figure 6 with the TDS system. The codes of the band-splitting system might be fixed or might be switched in synchronism with

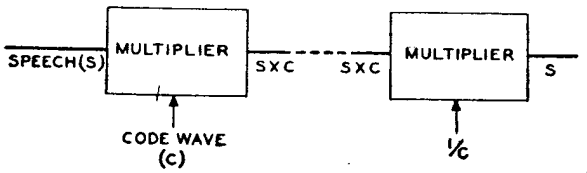



FIGURE 12. Multiplication system in which speech wave is multiplied by coding wave.

the TDS elements, the time scale of the scrambled speech not being further broken up. If they are switched nonsynchronously, however, the time dimensions will be further broken up, as will be seen subsequently. Combinations of nonrepeated code TDS and rapidly switched split-band coding can be made to afford a very high degree of privacy. The two kinds of coding, of course, must not be so interrelated that one furnishes clues for the other. If, for instance, a certain pole-piece were systematically associated with a certain split-band code the total privacy of the combination might be impaired rather than enhanced. A coding method for avoiding this difficulty is described in Preliminary Report[2] No. 21 of Project C-43.

A very special kind of scramble is produced by a system which consists functionally of Figure 6 (rapidly switched) in tandem with Figure 8 (with five bands) followed by an additional Figure 6. This is not the simplest form of the system, but it serves to illustrate the principle. Two frequency scrambles with a time shift in between produce a particular kind of two-dimensional scramble in which the speech is broken up into both time and frequency elements. Each of these elements may be shifted both in time and in frequency so as to be out of proximity with other elements with which they were originally associated either in time or in frequency. Another way of accomplishing this kind of scramble would be a combination of rapidly switched split band with a separate TDS system in each subband. A two-dimensional system was described in the Brown Boveri article[3] reproduced in Preliminary Report No. 5[4] and analyzed in Preliminary Report No. 9[5] of Project C-43.

For the sake of completeness two other sys-

tems involving time and frequency shifting will be mentioned, although as far as is known they exist only on paper. Suppose a sample of speech were recorded on tape and then reproduced at twice the normal speed. It would occupy only half the time it took to speak the words, but its frequency range would be twice the normal range. Let the upper half of the expanded frequency range be separated by a filter and modulated down to the normal range and used to fill up the unused time. The directly opposite but analogous system would involve reproducing recorded speech at half its normal speed; the frequency range would then be only half the normal range. Alternate sections, therefore, could be modulated up to fill the unused frequency space, thereby keeping the total transmitting time substantially unchanged. In both of these systems, there would be a delay equal to the length of one time element.

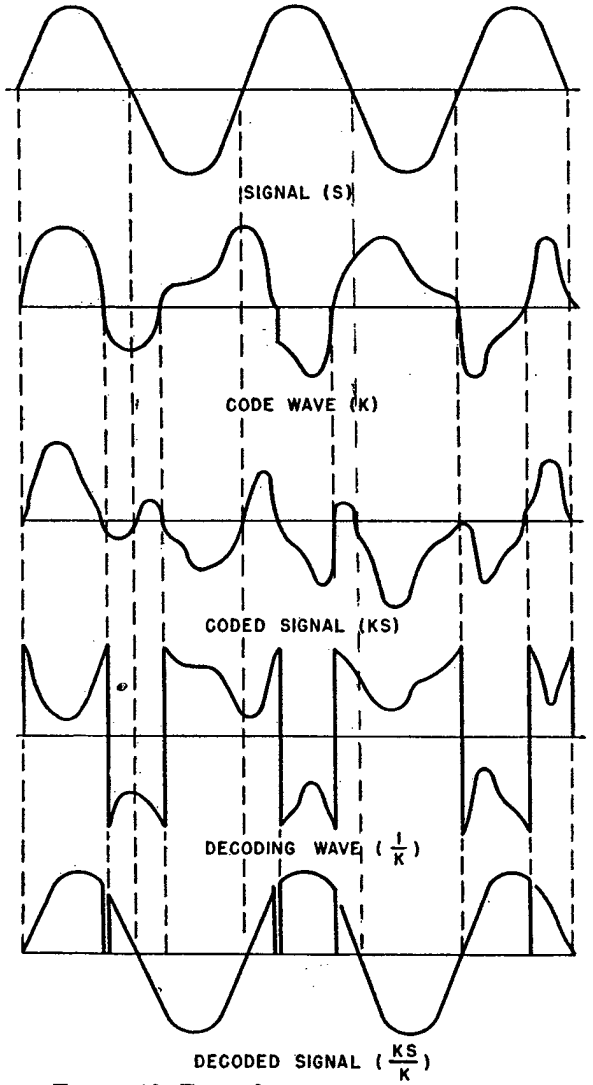



FIGURE 13. Example of multiplication system.

## 1.10 WAVE FORM MODIFICATION

Thus far we have considered systems in which frequency bands were shifted around or time elements were rearranged. There are a few privacy systems which make speech unintelligible by a direct modification of the wave form. One of these is shown diagrammatically in Figure 12. It depends upon a process whereby two waves are multiplied together, that is, the instantaneous amplitude of the resulting wave is the product of the amplitudes of the two input waves (not the *sum* or the *difference* as is the case in the simple inversion methods described above). One of the input waves to the multiplier is speech. The other is a complex coding wave. If the coding wave is sufficiently complex the resulting scramble is unintelligible. At the receiving end a reciprocal of the coding wave is derived and used as a multiplier, thereby restoring the original speech. Naturally, the coding waves at the two ends of the system must be in close agreement, otherwise there will be considerable background noise in the decoded speech. An example of the multiplication system is shown in Figure 13.

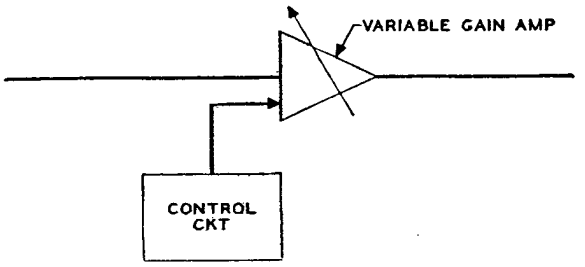



FIGURE 14. Level modulation; form of wave form alteration in which drastic changes in speech levels occur.

Another method for changing the wave form is shown in Figure 14. The essential feature of this system is an amplifier whose gain can be varied rapidly with time. Drastic changes

in the level of speech, if they occur rapidly enough, will make the speech unintelligible. The level changes might be made according to some program or they might be made to follow the

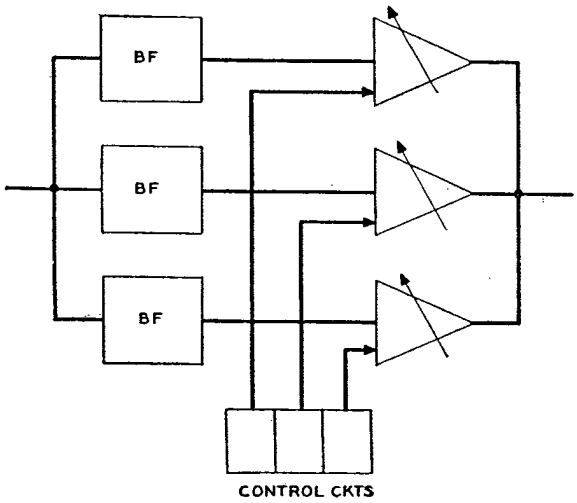



FIGURE 15. Level modulation system in which speech is first divided into subbands, each of which is subjected to level changes.

speech wave itself. For instance, extreme compression or expansion could be used. Corresponding gain changes, of course, must be made at the receiving end.

A variation of this system is shown in Figure 15. Here the speech band is first divided into subbands, and these are individually subjected to level changes according to separate programs.

use very high levels of masking signals to hide the intelligibility. This makes it difficult to subtract out satisfactorily: the difficulties are such that masking systems are more likely to be found on wire lines than on radio. A few speculative masking systems are outlined in the following paragraphs.

One form of masking system is shown in Figure 16. In this system, two telephone lines are used. At the sending end, noise is added to the speech in a mixing pad and the combination is sent over line 1. The noise alone is sent over a second line and is used at the receiving end to cancel the noise transmitted with the speech by simple subtraction. This system has the advantage that the noise can be completely random. However, since the enemy might tap both lines and thereby be able to make the same subtraction, a variation of this system consists in distorting the noise in some predetermined manner before sending it over the second line. At the receiving end, this distortion is first nullified so that the noise may be subtracted. Naturally, the form of distortion must be unknown to the enemy. It can, of course, be varied from moment to moment.

Another masking system is shown in Figure 17, which uses only one line. In this system, noise is added to the line at the receiving end instead of at the sending end. Again, the noise can be perfectly random. Since the noise is generated at the receiving end, the process of

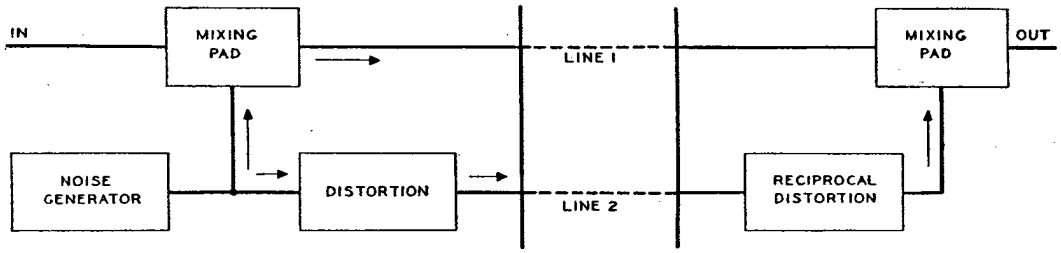



FIGURE 16. Noise masking requiring use of two telephone lines.

## 1.11 MASKING SYSTEMS

One of the first schemes which is likely to occur to a person considering how to make speech private is to add noise or other disturbing signal to the speech and remove it at the other end, in other words, to mask the speech. He will find, however, that it is necessary to

cancellation can, theoretically, be made very exact. This system, however, cannot be used for radio at all because the level of the noise decreases with distance from the receiver, while the level of the signal increases. The interceptor, therefore, will get good speech signals if close to the transmitter. With telephone lines this differential can be kept small.

Another simple masking system is to have a sequence of tones superposed on the signal at the transmitting end. At the receiving end,

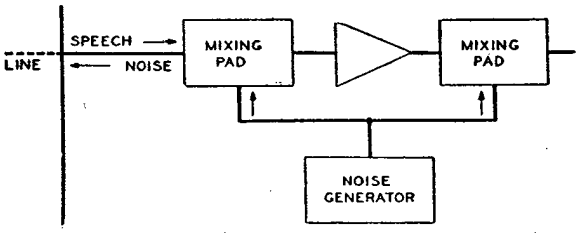



FIGURE 17. Method of applying masking noise at receiving end of communication circuit.

sharply tuned band elimination networks can be synchronously switched so as to remove the tones from the listener's ear. Similarly, short spurts of noise covering the whole frequency band can be applied at the transmitting end and shorted out at the receiving end. The spurts can be made to occur at irregular intervals according to a never repeating program. Both of these systems involve the loss of small portions of the speech, either in the time scale or the frequency scale.

A system described in Preliminary Report No. 4 of Project C-43 might be classified as a masking system, although it might be better classified as a means of communicating without the enemy's knowledge.

## 1.12 VOCODER SYSTEMS

The Vocoder system[6,7] may be made the basis for privacy systems of various kinds. The system is shown schematically in Figure 18. At the transmitting end the speech is passed through a series of band filters, the outputs

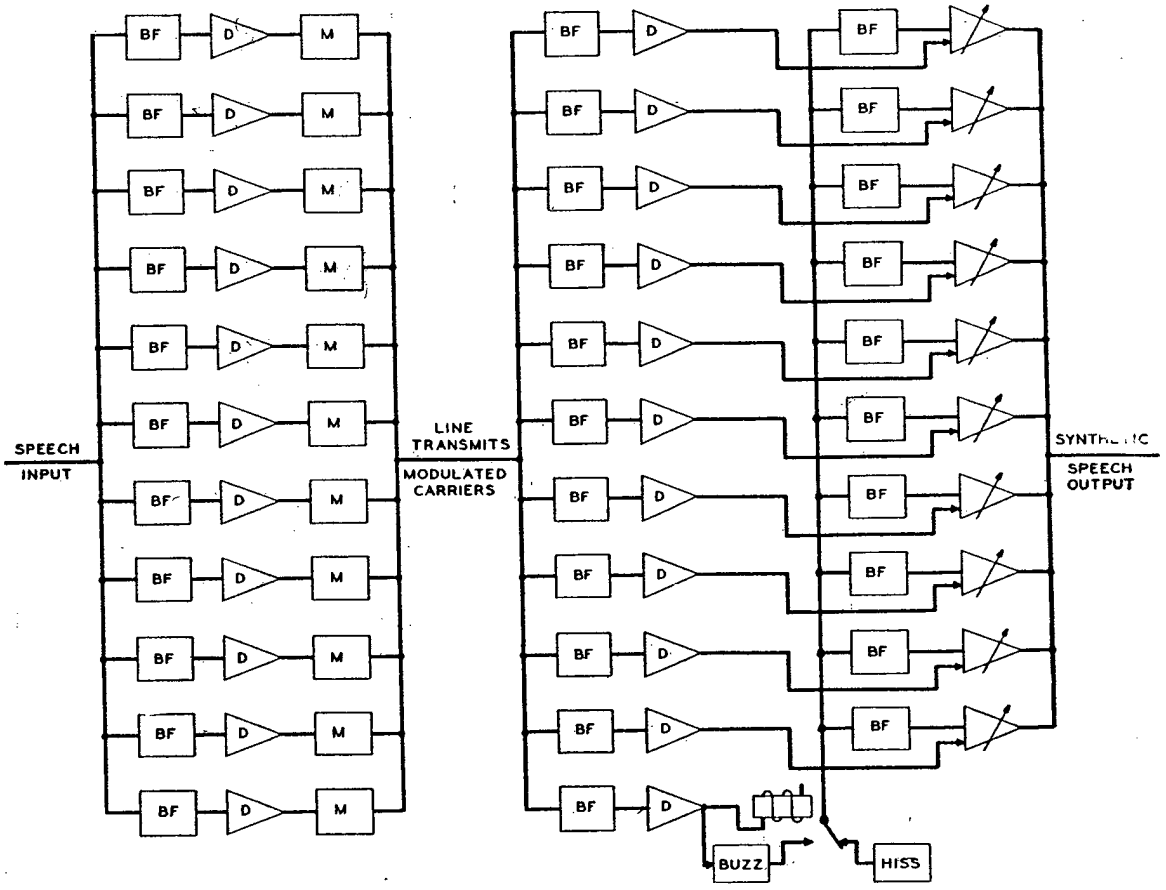



FIGURE 18. Vocoder system which may be made basis of privacy systems of various kinds.

of which are individually rectified to form a fluctuating d-c signal. These signals are individually modulated in such a way that they can all be sent over a single transmission path.

At the receiving end synthetic speech is manufactured in accordance with the signals transmitted over the line. A source of noise which covers the whole frequency range is passed through a set of band filters similar to those at the transmitting end. The output of each of these filters is controlled so that it is the same level as the level of the speech in the corresponding band at the transmitting end. This is accomplished by separating the signals in the various channels, detecting them and using the resulting fluctuating direct current to control the variable gain amplifiers in their respective channels.

The noise is of two types, depending on whether a voiced or unvoiced sound is to be simulated. For an unvoiced sound, it is a hiss-like thermal noise. For a voiced sound it is a buzz which consists of a series of harmonics covering the whole frequency range. A separate carrier is used to transmit information for operating this part of the system. At the transmitting end the pitch used by the talker is measured and this information is used to control the pitch of the buzz sound. The absence of a pitch signal switches the hiss sound into the system.

This system by itself, of course, is not private, since the enemy can build a similar system and use the signals to regenerate speech. Privacy must be achieved by operating on the channel signals. One method is to permute the channels at short intervals according to a prearranged program. Another method is to put a TDS system into the line, or into each channel separately. A still more effective method of this type is to apply a two-dimensional scramble, such as was described earlier, to the channels so that signal elements are displaced in both time and frequency.

## 1.13 CHANNEL-MIXING SYSTEMS

Thus far, the methods we have examined apply to a single transmission path. There is another class of privacy system which depends on using a multiplicity of paths. This is, of course, inefficient if only a single message is to be transmitted. However, the method can be applied to cases where a number of channels exist between two points and a number of messages would normally be transmitted over these channels simultaneously.

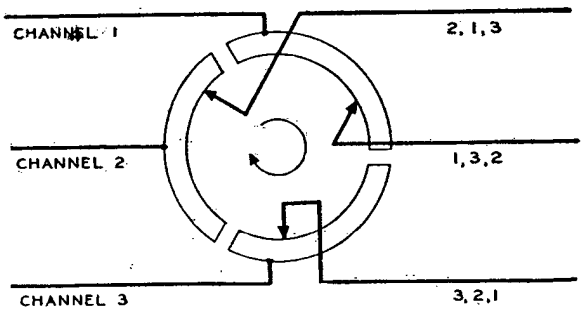



FIGURE 19. Channel mixing in which multiplicity of paths is involved.

Figure 19 shows one form of channel-mixing system. Here three channels are shown connected to the three segments of a commutator. Three brushes on this commutator are

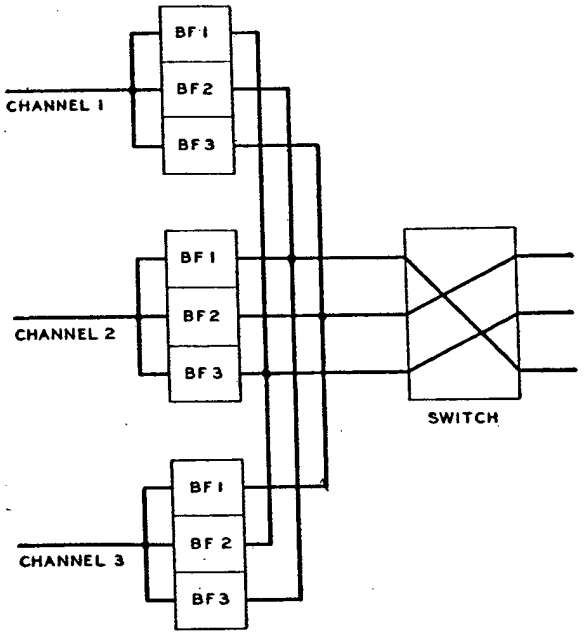



FIGURE 20. Subband channel mixing.

connected to the outgoing channels which are thereby caused to pick up one channel after the other on a time division basis. Each channel

contains parts of messages from all three channels. The commutator, of course, is too simple to be very effective and would, in practice, be replaced by a permuting switch capable of switching according to a more complex program. One or more of the channels may be filled up with the noise or spurious speech from a recording or other similar source.

An analogous system which divides the messages on a frequency basis is shown in Figure 20. Here each channel is passed through three band filters which divide the speech into subbands. Each of the outgoing channels contains subbands from each of the incoming channels. To increase the privacy, a permuting switch is shown which rearranges the subbands on a time division basis. If only one message is to be transmitted the other channels can be filled in with noise or spurious speech.

## 1.14 SUMMARY

The above examples cover fairly completely the range of schemes that might be used to scramble speech at audio frequencies. In subsequent chapters we will examine each system from the decoding standpoint. To facilitate reference to the various systems, they are summarized in Chapter 4, Table 1.

# Chapter 2

# TIME DIVISION SCRAMBLING SYSTEMS

## 2.1 INTRODUCTION

THE TWO MAIN DIVISIONS or characteristics of speech are the frequency dimension and the time dimension. Either or both of these components of speech may be rearranged or altered before or during transmission to insure privacy. At the receiver, the order of scrambling is reversed so that the original sense is recovered.

A privacy system developed to a high order during the war, known as time division scrambling [TDS], operates on the time characteristics of speech. In this system successive sections of speech, each $m$ seconds long, are divided into $n$ short time elements, and these $n$ elements are sent in a scrambled time sequence. The elements are much shorter than a syllable, so that each word is cut up and received as short bursts of energy in the wrong order.

All the summaries which follow deal with TDS systems.

## 2.2 PORTABLE TDS SYSTEMS—PROJECTS C-1 AND C-1A

While several forms of speech scramblers had been in use on radio circuits before 1940, there was none which was small and light enough to be suitable for mobile warfare. Work done in the summer of 1940 at the Bell Telephone Laboratories indicated that the need might be met in the form of time division scrambling by a small magnetic-tape recorder. The purpose of Projects C-1 and C-1A, therefore, was to investigate the possibilities of producing such a lightweight and effective privacy unit based on the TDS principle.

The fundamentals of this scheme were not new. It was known that such privacy should be very effective without appreciable expansion of the original frequency band, but the idea had not been developed for two reasons. First, it could not be used for commercial telephony because scrambling in time requires that the speech be stored for a certain time which introduced more delay than can be tolerated by inexperienced users. Secondly, there were several difficult technical problems that had not been solved.

Design ideas were collected by discussions with various specialists and a particular arrangement was visualized before the work was started. This set an objective and helped in segregating several problems that could be handled more or less individually and simultaneously. The more important of these included:

1. Development of a way to mount magnetic tape on the edge of a disk without introducing serious magnetic irregularities.
2. Development of a start-stop commutating arrangement for rapidly switching magnetic tape recorders and reproducers.
3. Development of a much more stable 24-volt motor drive than was then available.
4. Development of a compact amplifier unit to meet the special requirements of this system.
5. Development of a suitable switching arrangement for setting up scrambled combinations.

As the project progressed, the original design was changed where advisable and details were added. The five months set for completion of the project made it necessary to avoid any suggested changes that would appreciably delay the construction of models.

While development of experimental equipment was in progress, a separate group was investigating how various design factors would affect possible requirements for future equipment. These investigations were of two sorts. The first was concerned with the degree of privacy afforded by the equipment, and the second with factors affecting the final quality of the speech.

The degree of privacy was investigated as a function of the number of scrambling intervals within a cycle and the length of a cycle.

In this connection a rather thorough study was made of methods to "crack" the TDS privacy under conditions ranging from limited facilities and personnel to extensive laboratory equipment handled by experts. The conclusions were that cracking was rather unlikely unless attempted by experts with special equipment, and in this latter case the five-unit design developed for experimental use might be cracked within minutes. In spite of this, it was believed that the five-unit design would be very effective when used on radio telephone circuits for the direction of maneuvers that are completed within minutes. This would suggest use for such links as plane-to-plane, plane-to-ground, and tank-to-tank.

The investigations concerned with speech quality included such things as the way in which accuracy of synchronism, start-stop brush operation, and the position of various elements associated with the scrambling and reconstruction process affected the final quality of the speech. The most important conclusion here was that the degree of stability afforded by the special motor designed for the experimental TDS unit met the requirements very satisfactorily. The indications were that it would not be difficult to provide a final design which would introduce little degradation.

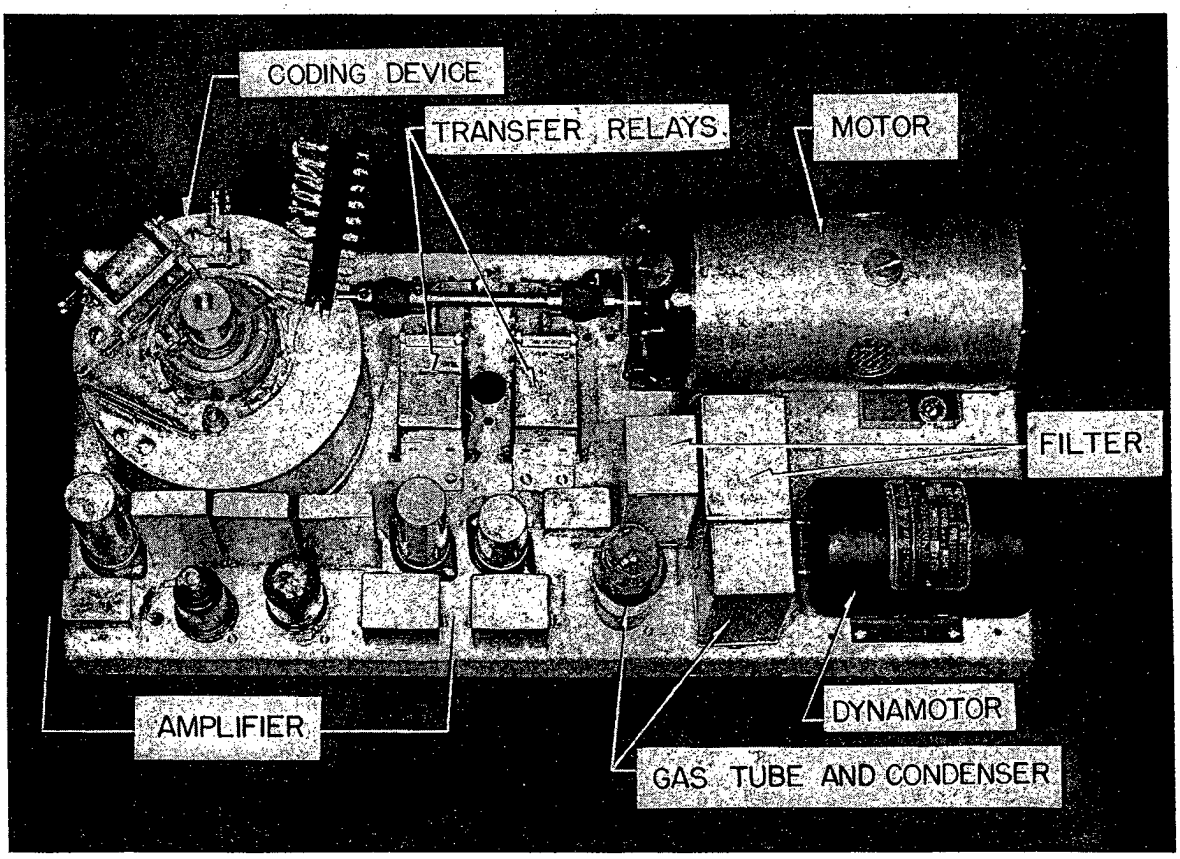



FIGURE 1. General view of TDS system developed under Project C-1.

With the experimental TDS unit produced during the project about fifty useful combinations could be set up on the five front-panel dial switches. When used in association with radiotelephone equipment, connections were required to the transmitter, receiver, and power supply. The system used 100 watts at 24 volts, but would operate over a voltage range of approximately 22 to 30. The weight was about 40 lb and the dimensions were 7¾ in. high, 9 in. deep, and 20 in. long.

2.2.1

## Demonstrations

In March and April 1941, four experimental TDS units were demonstrated in Washington before members of the National Defense Research Committee [NDRC] and representatives of the Army and Navy. The units were set up first in separate rooms at the Carnegie Institution and later one unit was set up in the Navy Building and another in the Munitions Building with connections to telephone extensions in both places. The equipment was demonstrated to representatives of the Army and Navy as well as to members of the British Military Mission and the Canadian Air Ministry.

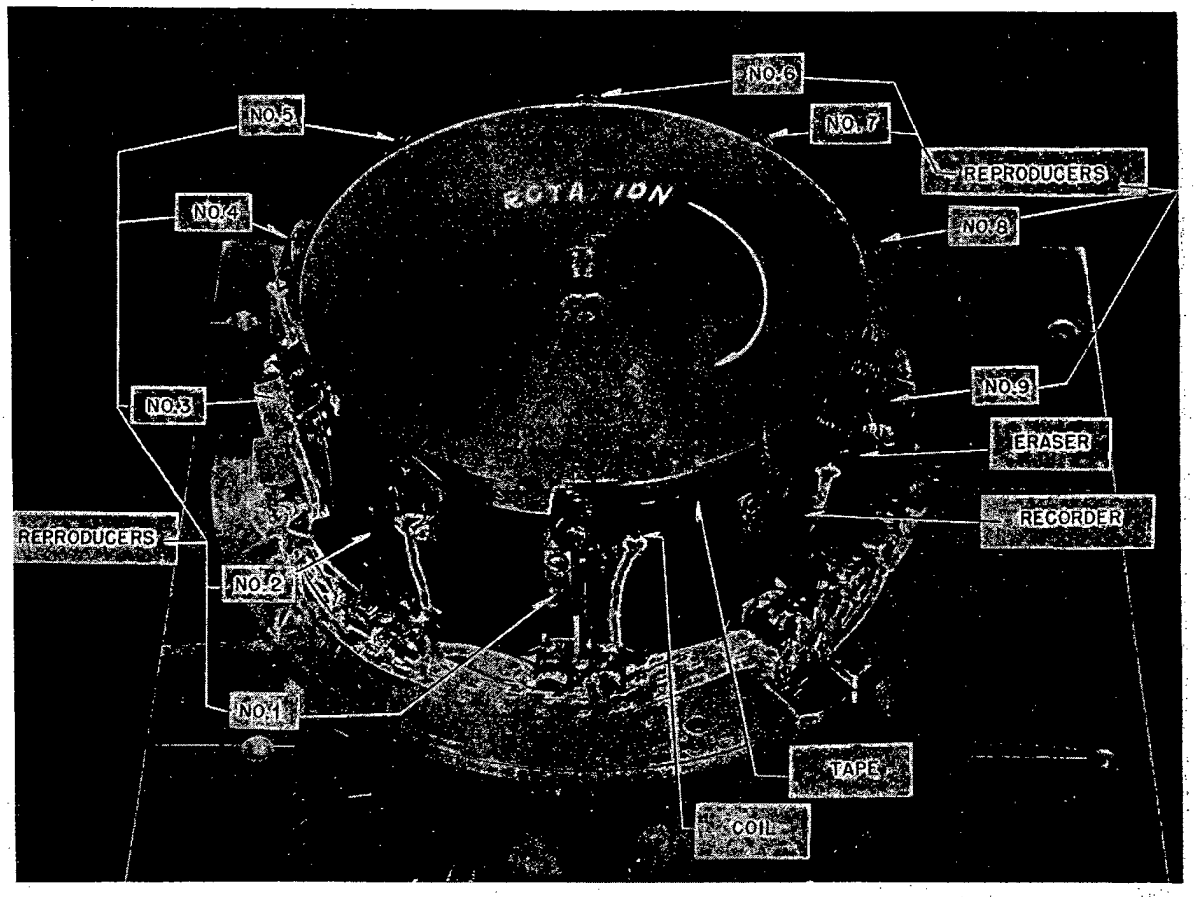



FIGURE 2. Tape wheel of C-1 TDS unit showing placement of individual reproducers, etc.

2.2.2

## The TDS Units

The essential part of the TDS units consists of the magnetic recorder-reproducer made up of a drum or wheel on the periphery of which is mounted a wide magnetic tape alloy. Around the wheel and in contact with the tape are eleven pole-pieces, mounted so that all traverse the same narrow band of the tape. The pole-pieces comprise one eraser supplied with direct current for magnetically saturating the tape to obliterate previous recordings, one recorder supplied with speech current, and a 1-ma d-c depolarizing current and nine reproducer pole-pieces spaced 36 degrees apart.

Associated with each reproducer pole-piece is a segment of a commutator and a contact to a switching system so that the order in which the recorded speech currents are taken off for transmission by radio or wire can be changed from the order in which the recording was made.

The intervals of speech each 0.30 sec long are divided into five sections of 0.06 sec dura-

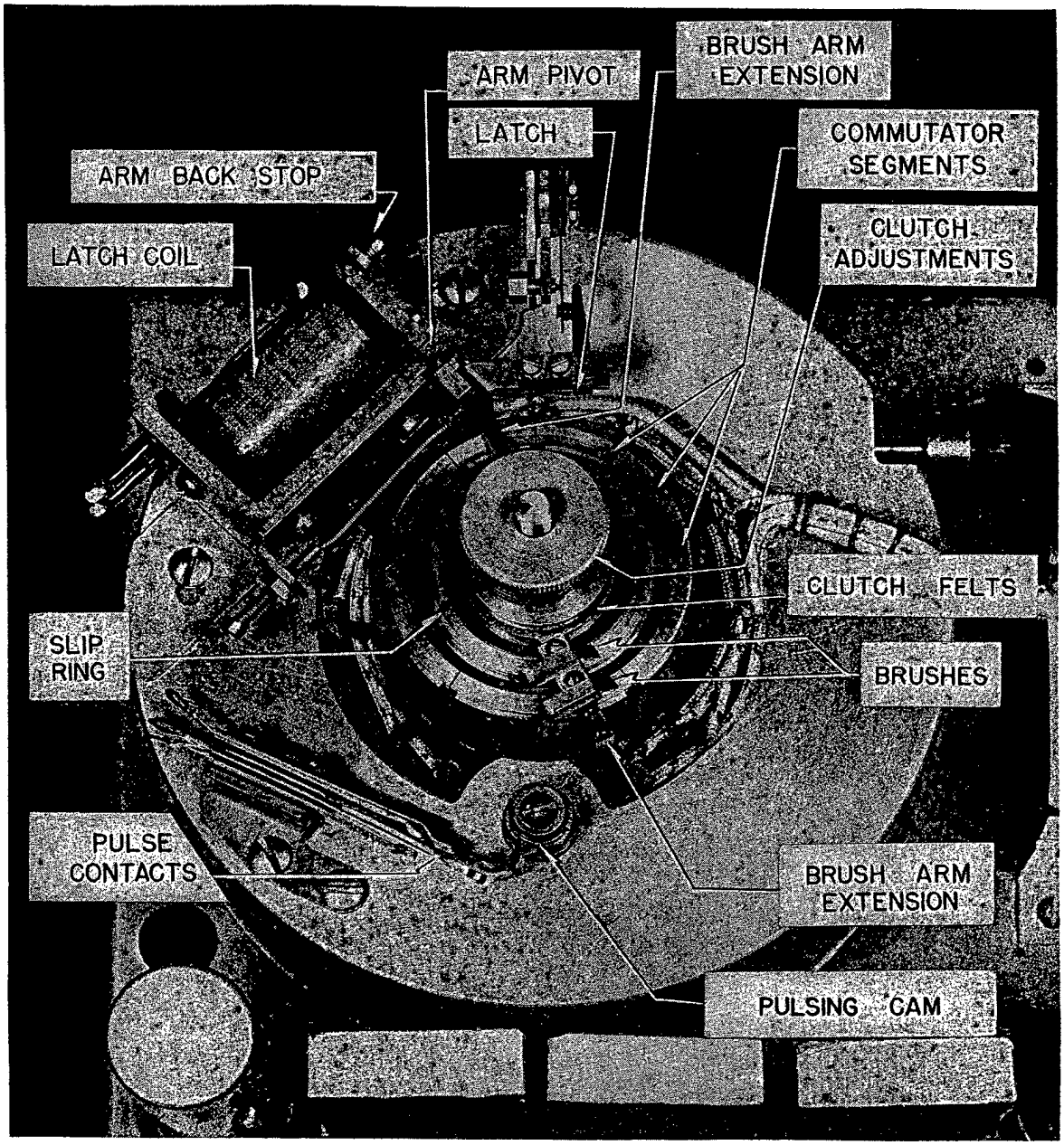



FIGURE 3. Commutator details.

tion. The instrument is described in considerable detail in the final reports of the project.

The final report[8, 9] of Project C-1A, a continuation of Project C-1, describes methods of cracking the TDS system, gives an estimate of the time required to crack it, an evaluation of the privacy secured by it, and recommendations concerning future developments, some of which resulted in Projects C-50 and C-65.

### 2.2.3 Conclusions

The project demonstrated that TDS could provide a useful degree of privacy in a portable

device of reasonably small dimensions and weight. Further developments to meet military needs were pursued by the Services themselves. The problem of speech privacy was attacked in other NDRC projects along many other lines, as evidenced by summaries of other Division 13 projects in this volume, but to the end of the war TDS remained the only small and portable device for scrambling speech that was in factory production.

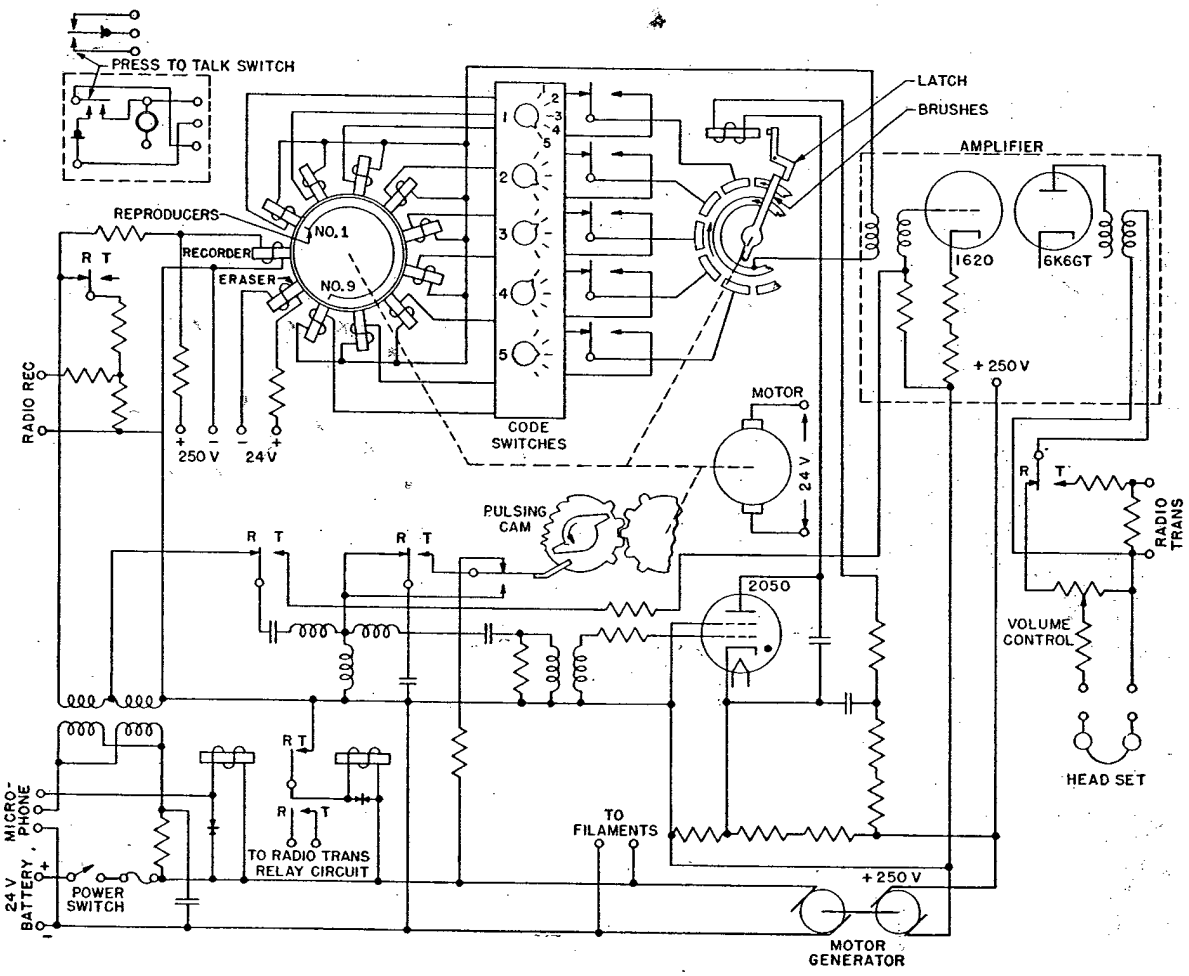



FIGURE 4. Simplified circuit diagram of C-1 TDS system.

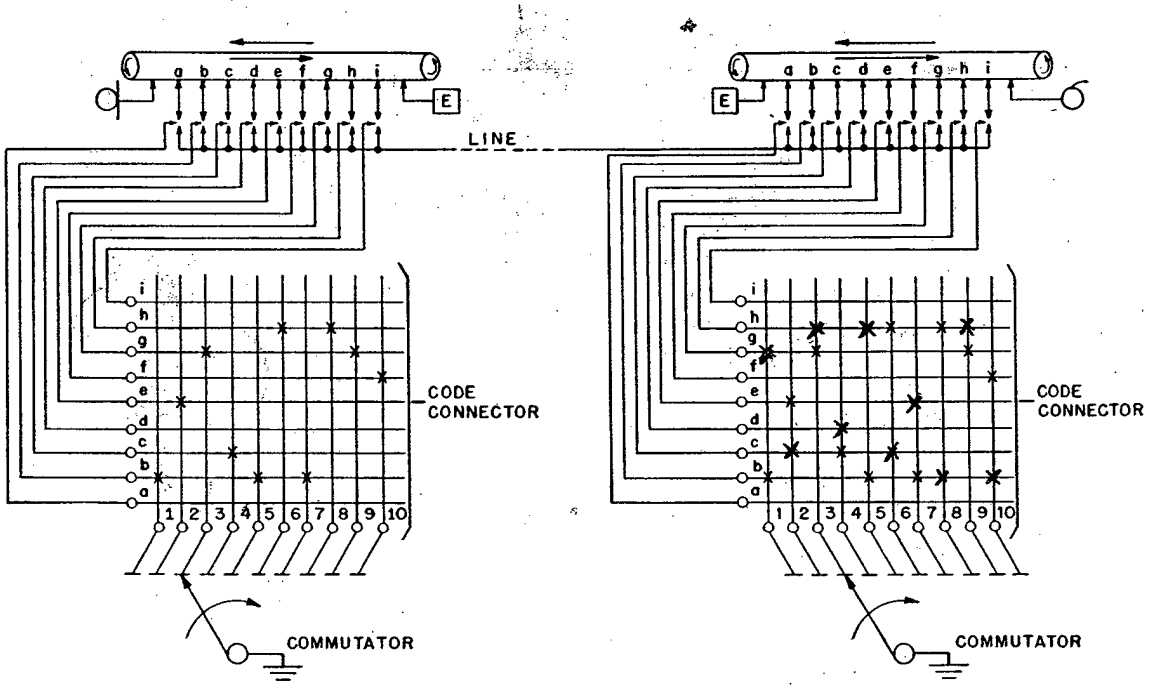
## 2.3 CONTINUOUSLY CODED TDS—PROJECT C-50

The report on Project C-1A suggested an improvement of security provided by TDS equipment by provisions for automatic code changing every code cycle. In the winter of 1942 means for doing this were suggested and Project C-50[10] was set up to develop these means. The specific object was to provide model equipment so that the privacy obtained by elaborating the TDS principle to its practical limit could be studied.

In the manually operated TDS system, the nine pole-pieces which "take off" the recorded segments of speech are connected to a commutator and switch by which the operator can change the order in which the successive elements are transmitted to the lines or to a radio transmitter. The object in using different ones of the various pole-pieces is to retard or delay successive elements of the recorded message or

speech by different amounts. When two speech elements which were originally in succession are delayed by different amounts they are displaced in time with respect to each other. They may be merely interchanged with respect to each other or they may be separated widely by inserting other speech elements between them.

The scrambled speech elements are returned to their proper order in the unscrambling process by delaying each one in a selective manner so that the total delay contributed by scrambling and unscrambling is the same for each element. Elements scrambled with minimum delay are unscrambled with maximum delay, and vice versa. The speech, when reassembled, has been delayed by the sum of the minimum and maximum delays. In the C-50 TDS system this total delay is 700 msec.




Code used is:

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Commutator bars | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Speech units | 4 | 2 | 1 | 6 | 8 | 3 | 10 | 5 | 7 | 9 |
| Coils | b | e | g | c | b | h | b | h | g | f |

FIGURE 5. TDS coding connections. Transmit machine codes on "reproduce," while receive machine decodes on "record."

### 2.3.1 The C-50 TDS System

In the TDS units developed under Project C-1, there were nine take-off pole-pieces, a recording pole-piece, and an erasing pole-piece. In the C-50 TDS system, each pole-piece is capable of recording, of erasing, and of reproducing. Such a system is known as a ten-element system because ten speech elements are scrambled in each code cycle. In the C-50 system, two interlaced ten-element codes are employed in each code cycle.

If the interconnection of pole-pieces and commutator segments remains fixed, the code or key is fixed and the transposition scheme is repeated with each revolution of the brush over the twenty commutator segments. This takes place in 750 msec. By means of punched code cards, the C-50 TDS system can be operated in this manner, if desired.

### 2.3.2 Continuous Coding

The continuous coding equipment makes two changes in the interconnection of pole-pieces to segments in each revolution. The connections to odd-numbered segments remain fixed until

the commutator brush leaves the nineteenth segment; when the brush starts on segment No. 1 an entirely different set of interconnections is used in the next revolution by the odd-numbered segments. The pattern for the even-numbered segments begins with the twelfth segment and extends around the commutator through the tenth segment; when the brush reaches the twelfth segment again a new pattern is ready for the even segments. In this way the coding for alternate segments constitutes two independent systems of transpositions, each changing every 750 msec but displaced from each other by 375 msec.

The odd-numbered and the even-numbered commutator segments can be treated separately because the time taken for the brush to cover one segment, 37.5 msec, is exactly half the time required for the magnetic tape to move from one reproducing pole-piece to the next. The portions of speech available for reproduction when the brush is on odd segments are, therefore, never available when the brush is on even segments.

The patterns of interconnection between pole-pieces and commutator segments must follow certain rules in order that the TDS generate a transposition which is valid, in the sense that each speech element is transmitted once and only once. Since speech on the magnetic tape remains there as it goes past all nine reproducing pole-pieces, a random choice of reproducing pole-pieces might pick up the same element of speech twice or more, and some other element would be omitted for each repetition.

The kinds of interconnections which give

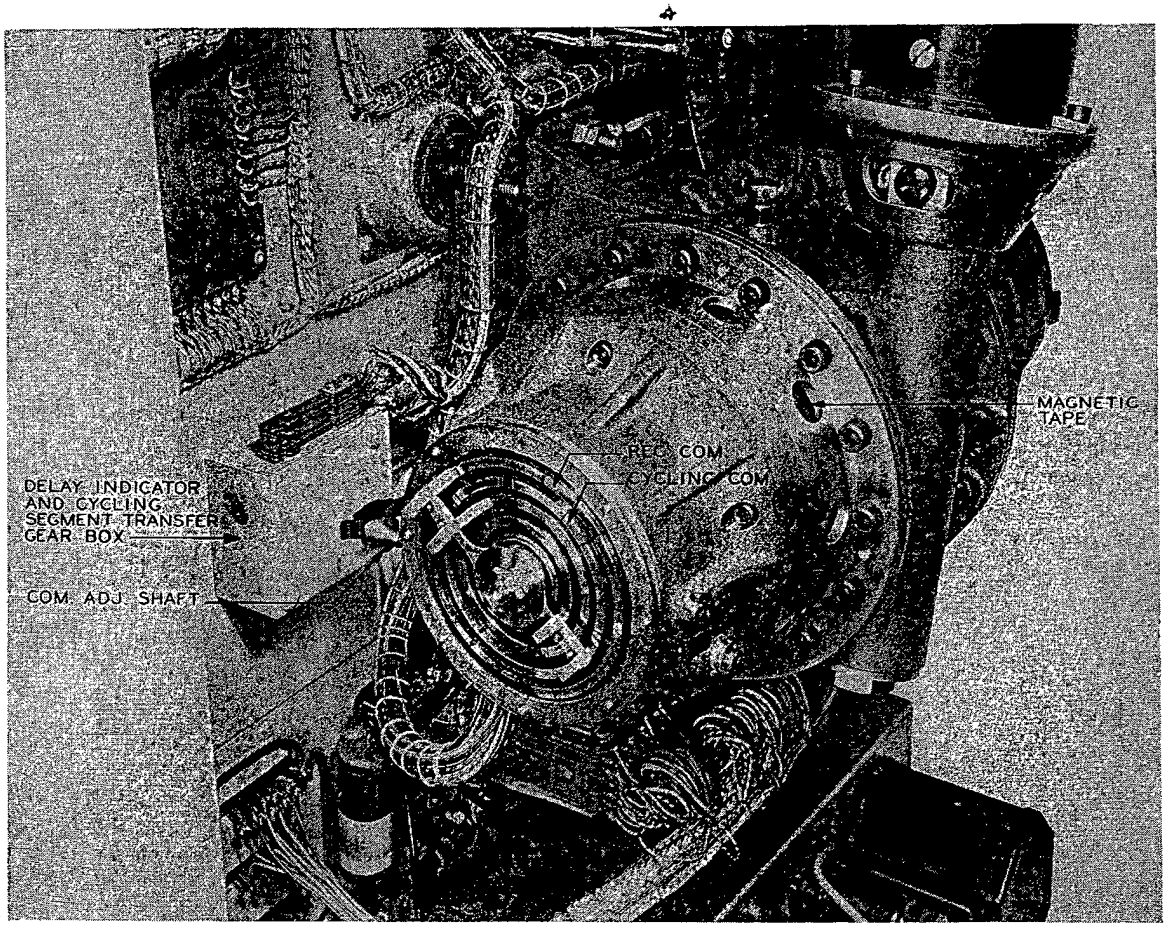



FIGURE 6. Details of C-50 TDS machine.

useful codes are discussed in Appendix A of the project final report. The rules worked out in that appendix are basic in the design of the automatic coding apparatus which must be so arranged that the semirandom series of choices called for in one part of the coding equipment is scrutinized in another part and revised until the interconnection finally set up is a valid transposition.

### 2.3.3 Number of Codes Available

The complexity of the coding systems generated by the automatic coding equipment in the C-50 TDS may be illustrated by the fact that there are 1,625,702,400 different sequences of codes for each of the two interlaced systems or the square of this figure for the combination. The choice of the particular sequence to be used is governed by four punched cards. The initial settings of ten selector switches then determine the point in the sequence at which the sequence will start. There are $(3,282,972)^2$ such starting points for each sequence.

From the point of view of those operating the equipment, the four punched cards and the ten selector switch settings constitute the key, since these choices must be agreed upon at both ends of the circuit.

When the cards and initial settings have been chosen, the equipment can be started, after which it provides in each of the interlaced systems, an irregular order of valid codes from a possible number of 60,316 codes. In a single message, or even in a whole day's use with the same initial settings, only an extremely small fraction of any code cycle would ever be used. Each particular sequence runs so long that it would not begin to repeat before 6,400,000 years.

### 2.3.4 C-50 TDS Plus Frequency-Band Switching

Although to the end of the project, decoding methods developed under other Division 13 projects failed to crack the C-50 system, it was found that some trained individuals under favorable circumstances were able to understand some of the scrambled speech. Less is understood with fast talkers than with slow talkers but the amount understood by such trained observers at normal speech rates leads one to the conclusion that in a system intended to provide long-term privacy the TDS principle should not be used singly but in combination with other principles.

A combined system should be so devised that direct listening is of no value and should be arranged so that an intercepter can not disentangle the two types of scramble and obtain intelligence by listening directly to one of them. Such a system is provided by the C-50 TDS combined with and controlling a rapidly switched frequency-band shift system (A3) so arranged that the C-50 TDS coding equipment controls the sequence of A3 codes. In this arrangement the A3 codes may be switched as often as every 37.5 msec. No useful intelligence had been extracted from the resultant scramble in direct listening tests up to the time the final report on Project C-50 was written. Furthermore the difficulty of decoding the scrambled speech by other methods was expected to be materially increased. Although the combined C-50 TDS and A3 systems weighed about 2,200 lb and required a power of 1,500 watts, its probable privacy and its availability were such as to be recommended for use in corps-to-division communications and in similar Navy situations. This double scramble system is described in Appendix F of the final report of Project C-50. Actual work on such a system was carried out under Project C-66.

### 2.3.5 Appendices to Report of Project C-50

The following titles of the several appendices to the final report of Project C-50 give an indication of the material to be found in the report itself but not summarized here.

Appendix A Basic TDS Principles
Appendix B Automatic Code Generating
Appendix C Number of Codes and Code Sequences
Appendix D Detailed Description of C-50 Equipment
Appendix E Operating Instructions
Appendix F C-50 and A3 Systems Combined
Appendix G Project C-50 Drawings

## 2.4 FREQUENCY-TIME DIVISION SYSTEM—PROJECT C-66

In 1942 it was known that the speech security provided by the TDS units developed under Project C-1 was short unless automatic coding was used as developed in Project C-50. It was known, too, that only short-time security was provided by the A3 scramble based on permutations of frequency bands. There was reason to believe that A3 in tandem with TDS might provide a much higher order of security and Project C-66[11] was set up to study this.

### 2.4.1 Accomplishments of the Project

It was found that A3, switched even as often as every 60 msec, in tandem with the portable fixed-code TDS, gave an increase in privacy incommensurate with the circuit complexity. When rapidly switched A3 was combined with the continuously recoded TDS of Project C-50, however, the degree of security attained appeared to justify recommendation of the development of the combination for truck-mounted use in corps-to-division communication. So far as is known, this recommendation was not acted upon.

The actual security and the transmission features of the combined systems may be summarized as follows:

1. Although it is possible under some circumstances for trained observers to obtain some intelligence from listening directly to the scrambled speech from either A3 or C-50 systems alone, when these are combined practically no intelligence can be obtained from the scrambled speech in this manner.

2. The unauthorized agent would require special and complex analyzing equipment to restore the scrambled speech from the combined systems. The cracking time had not been determined on the date of the final report (May 29, 1943). The C-50 TDS alone using nonrepeating codes had been found very difficult to crack in a form permitting reproduction of the message, and it was the opinion of the personnel of Project C-43 (which was largely concerned with cracking methods and which became expert in this technique) that the cracking of this TDS in combination with and controlling the A3 would be much more difficult, since the A3 codes obscure the matching of the speech elements. Even if this can be done successfully there appears to be a major development problem with respect to reproducing the message from the reassembled photographic traces.

3. The C-50 TDS plus A3 provides transmission quality of a useful grade. Under limiting conditions, however, the signal-to-noise ratio must be about 7.5 db greater than that required when the privacy system is not used. Under average conditions articulation tests showed that the C-50 TDS plus A3 system was equivalent to a reference circuit without privacy having a bandwidth from 250 to 3,000 cycles and a signal-to-noise ratio of about 14 db.

### 2.4.2 Other Studies under Project C-66

The transmission quality of devices combining frequency scrambling with time delays provided by means of magnetic tape was found in this investigation to depend upon control of the following factors:

1. Modulation products giving rise to nonlinearity.
2. Flutter from speed variation in magnetic tapes.
3. The signal-to-noise ratio of the overall system.
4. The transmission frequency characteristics.
5. Switching effects.

Detailed analyses of these controlling factors are found in the final report of the project.

Among other systems and schemes for obtaining privacy by time and frequency scrambling considered in the course of Project C-66, the following deserve mention:

1. A re-entrant frequency band shifter.
2. A two-dimensional scrambler employing frequency band delay plus a re-entrant frequency band shifter plus frequency band delays.
3. A two-dimensional scrambler employing a re-entrant frequency band shifter plus fre-

quency band delays plus a re-entrant band shifter.

4. A two-dimensional scrambler employing A3 privacy and five magnetic-tape delay circuits of different delay values.

tion expires. If a mission of mobile units takes a greater time than this protected period, changes in the code should be made during the mission. Only enough codes should be available to afford the desired protection. More codes than necessary would provide the enemy with too much information if a unit were captured.

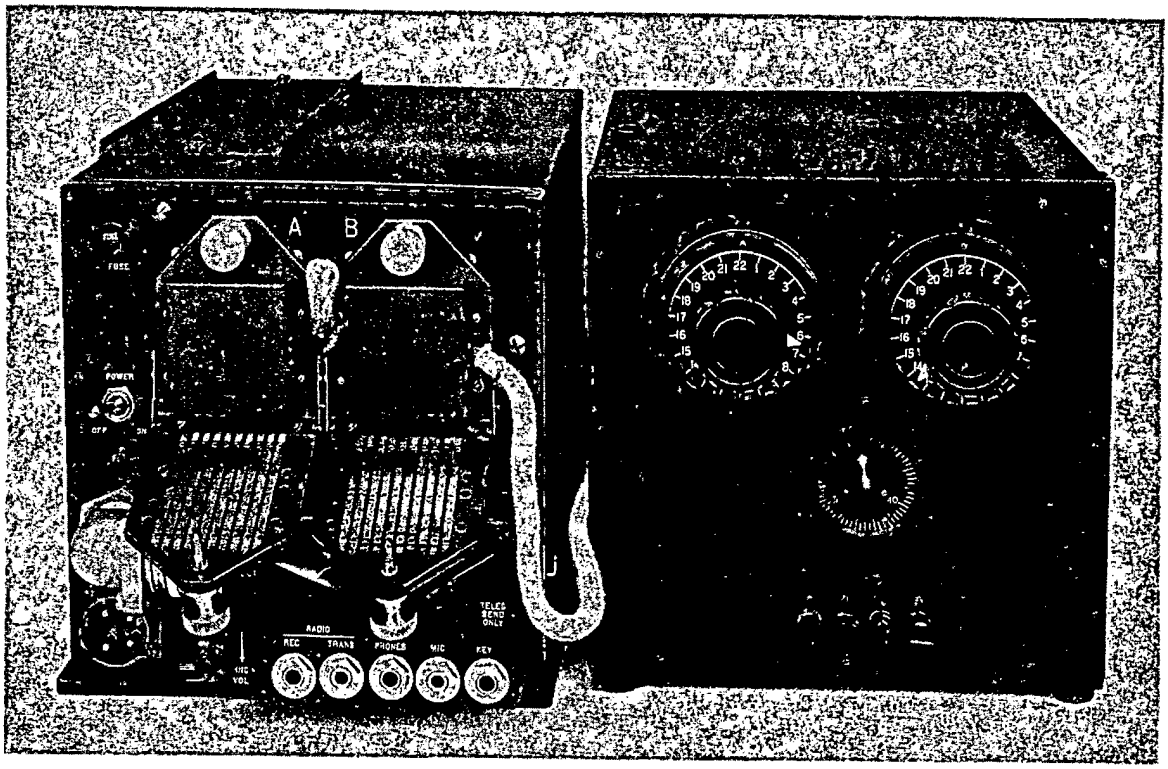



FIGURE 7. Exterior view of Model B code-changing unit attached to D-150285 TDS unit.

## 2.5 CODE-CHANGING ATTACHMENT FOR THE C-1 TDS UNIT—PROJECT C-65

The final report of Project C-1A suggested that the security of the TDS speech scramblers would be improved by frequent changes of code cards. In 1942 a variety of means had been suggested for accomplishing this by an attachment to the TDS unit (D-150285) then being produced for Army and Navy. Project C-65[12] had as its purpose the development of such an attachment. The background for this work is as follows:

Since the security afforded by fixed-code privacy systems cannot be relied upon beyond the period required by an unauthorized intercepter to work out the code, it is desirable to change the code before this minimum period of protec-

Under the stress of the circumstances attending an actual mission, the changing of codes might be neglected unless the operation is fully or partially automatic. If only partially automatic, the operation should require only simple and positive motions, such as pushing buttons or pulling levers, to be carried out on command.

Two designs were selected from the many considered and two units each of these designs have been constructed. One design provides for electrical operation under control of a timer, though manual operation is possible; the other design is arranged for manual operation but could be converted to automatic operation by further development. The correctness of the operating principles has been checked by tests

on TDS units. Choice between the two will depend on military requirements and manufacturing considerations.

The two models are functionally equivalent since each provides a choice of twenty double codes, and the particular sets of twenty from the several hundred available may be changed between missions. In the automatic model, codes are set up by means of ninety small relays, controlled by contacts made through two perforated

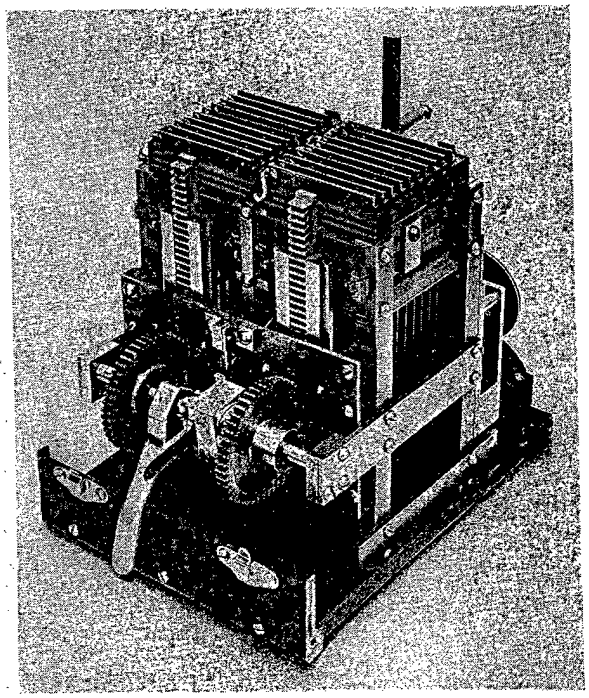


FIGURE 8. Model C code-changing unit with case removed; back and top view.

sheets, similar to player-piano rolls, with twenty codes per sheet. In the manually operated model, a mechanism pushes two code cards, out of two groups of twenty contained in loading boxes, to close two sets of spring contacts according to the arrangement of perforations in the code cards.

The automatic model operates on 24 volts, drawing 0.8 amp between changes and 1.5 amp during changes.

The automatic model is about 10 per cent less than the TDS unit in cubic contents, and, for comparable materials, of about the same weight. The manual model has about half the volume and, for comparable materials, about half the weight of the TDS unit. Both models could be operated by a single motion of a gloved hand.

## 2.6 TELEGRAPHY APPLIED TO TDS—PROJECT C-55

Project C-55[13] was undertaken at the request of the Signal Corps early in 1942 to determine the advantages and disadvantages (if any) of incorporating means for tone telegraphy in connection with TDS equipment which had been developed for the Services. At the same time the question was raised as to whether the use of telegraph might not jeopardize the privacy of the device for speech. This was based on the idea that the TDS code might be recovered more quickly from scrambled telegraph signals than from scrambled speech signals. It was important to answer this question to determine whether restrictions would be needed on the use of telegraph.

The questions to be answered may be summarized as follows.

1. Is TDS privacy less for telegraph than for speech? That is, will the use of telegraph

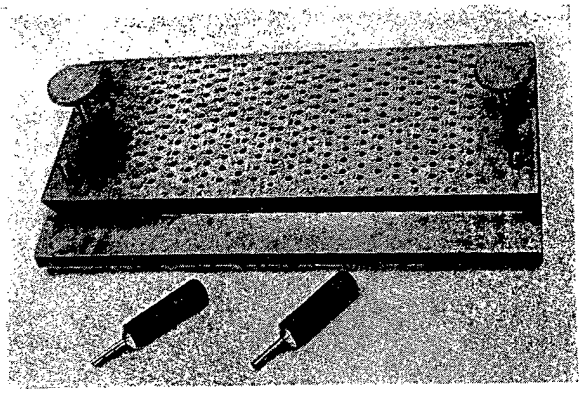


FIGURE 9. Model B die for punching code masks.

through TDS tend to expose the code and thus reduce the privacy for subsequent telephone use?

2. Is TDS privacy for telegraph critically dependent upon rates of hand sending and lengths of TDS time elements?

3. What impairment to telegraph transmission is caused by TDS?

4. Is it feasible to apply machine telegraph sending to TDS?

With regard to the relative privacy of telegraph and speech, the data if taken literally indicate a slightly greater privacy for telegraph than for speech. The differences in the average solving times are so small as to be negligible, however. The solving times both for telegraph and speech vary from sample to sample, so that some telegraph samples were solved more quickly than some speech samples, but the opposite was likewise true, and the range of variation was about the same for telegraph and speech.

However, there is a difference of another nature which is inherent. The two main steps in the restoration of scrambled speech are, first, that the code be found and, second, that the scrambled speech be reproduced through TDS equipment arranged for the unscrambling code. These steps also can be used for unscrambling telegraph, and if they are used there is no difference in the degree of privacy for speech and telegraph, since the times taken to ascertain the codes were the same. But another method might also be used for telegraph. If an oscillogram or a paper trace were made of the entire scrambled message, then solution of the code would supply the formula according to which trace should be cut up and reassembled. If this were done for speech, the result would still be unreadable without fairly elaborate equipment; but a reassembled telegraph trace could be read by visual inspection of the dots and dashes.

As a practical matter this difference appears to be of little importance, as the following calculation indicates:

At 25 words per minute, a 100-word message takes 4 min, or 240 sec. At 0.75 sec per TDS cycle, this would cover $\frac{4}{3} \times 240 = 320$ TDS cycles, or supply $20 \times 320 = 6{,}400$ TDS elements for manipulation. If the trace were run so as to allow $\frac{1}{4}$ in. to each element, or 48 elements to the foot, which would be extremely compressed, the trace would need to be 6400/48 = 133 ft long. Even with practice and concentration probably at least a minute would be needed to reassemble each cycle, what with the manual labor of cutting and pasting, or 320 min in all; that is, it would take about 5 hr for one person to recover a 4-min message. Additional people or supplementary equipment would, of course, reduce this time.

Thus, while the sense of the telegraph message can be recovered with less elaborate equipment than is needed for speech, the amount of clerical work involved would constitute a protection lasting longer than the privacy time which should normally be associated with a fixed-code system.

The answers to the questions posed above were found to be about as follows.

1. Scrambled hand-sent telegraph signals require at least as much time to decode as scrambled speech; there is therefore no reason to believe that the application of manual tone telegraph to TDS will jeopardize its value for speech.

2. The privacy of TDS for telegraph is not critically dependent on rates of hand sending and lengths of TDS time elements.

3. The limits of telegraph transmission are reached with about 5 db less thermal (random) noise with the TDS than without; this means that the range is reduced unless the signal strength is increased. The impairment is less for short elements than for long TDS time elements.

4. Machine telegraph, both Boehme and teletypewriter, give generally legible, though not letter-perfect, results with single-tone transmission, if care is used. Better results, though still not perfect, may be obtained with two-tone transmission.

The final report[13] of Project C-55 covers the individual points raised in the above questions in considerable detail and includes additional material, not summarized here, on the question of the quality of hand or machine sending as affected by TDS.

# Chapter 3

# SPEECH PRIVACY SYSTEM DEVELOPMENT

## 3.1 RCA-BEDFORD SPEECH PRIVACY SYSTEM

IN THE RCA-BEDFORD speech privacy system,[a] a portable system having short-term security, the speech wave is coded by multiplying it by an audio-frequency coding wave. A connecting circuit between transmitter and receiver having essentially faithful reproduction over a band of 100 to 4,000 cycles furnishes the required intelligibility and reliability.

### 3.1.1 Basic Principles

At the sending end a sound wave $S_0$ is first "compressed" to a uniform average amplitude level by a special compandor circuit to form a signal $S$. The signal $S$ is then multiplied by a suitable audio-frequency coding wave $K$ to form a coded wave $SK$ which is unintelligible. The expression "multiplied," as herein used, means that the product wave $SK$ has instantaneous ordinates measured from its a-c axis which are proportional to the corresponding products of the original waves $S$ and $K$. This is illustrated by waves $S$, $K$, and $SK$, Figure 1.

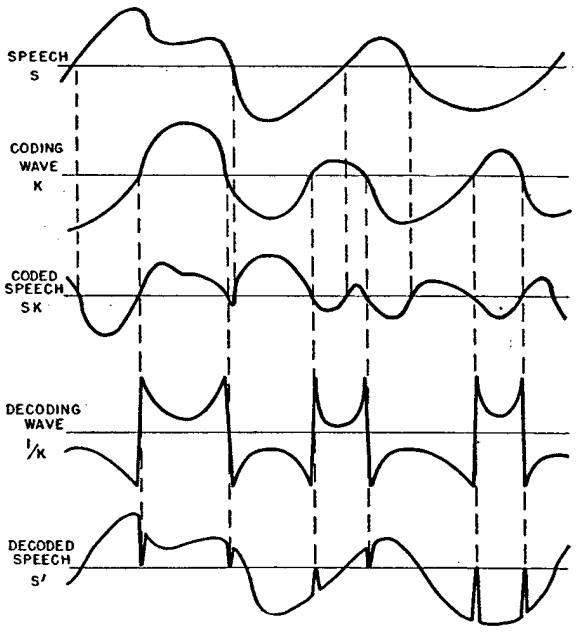



FIGURE 1. Coding and decoding processes involved in RCA-Bedford multiplication privacy system.

At the receiving end the coded wave $SK$ is multiplied by the "reciprocal" wave $1/K$ (which is derived from the locally generated code wave $K$) to produce the restored speech wave $S'$, which is ideally like $S$.

$$SK \times \frac{1}{K} = S \text{ or } S'.$$

As shown in Figure 1, the reciprocal wave $1/K$ has instantaneous ordinates which are proportional to the reciprocal of the corresponding coding $K$.

The ordinates of the coded wave $SK$ become zero each time the coding wave becomes zero. For these instants the reciprocal wave $1/K$ ideally should become infinite. Since this is impossible in practice, a narrow gap must occur in the restored wave $S'$ as shown in the figure, at each time the wave $K$ passes through zero. This amounts to an introduction of spurious signal components, which are largely removed by a low-pass filter.

The decoded wave $S'$, which is still compressed, is "expanded" to its original level by the receiving end of the compandor. The expanded signal $S_0'$, which is like $S_0$ except for losses, is heard in the phones.

The various treatments of the signal are indicated in the block diagram, Figure 2.

### 3.1.2 Wave Multiplier

The wave multiplier used to multiply audio-frequency waves $S$ by $K$ and $SK$ by $1/K$ is really a balanced modulator which is completely "balanced" in the sense that only the instantaneous product terms are produced. This balanced condition can also be described by saying that the output contains only the sideband frequencies

[a] Project C-54, Contract No. OEMsr-592, Radio Corporation of America.

of modulation; namely, those frequencies which are the sums or the differences of the frequencies of $S$ and $K$. Ideally, no harmonics of either $S$ or $K$ are present in the output. This is an important fact from the standpoint of security.

This process would correspond to modulation as commonly used in radio transmission, except that in the privacy system, both the carrier and the speech waves are suppressed. In radio this can be accomplished in an unbalanced modulator followed by filters to suppress the undesired frequencies. The present multiplication process could not be carried out in this manner because the frequencies it is desired to suppress occupy the same frequency range as the desired modulation sidebands.

The special wave multiplier developed for the speech privacy system employs four small oxide rectifiers (known commercially as varistors) operating in their square law range.

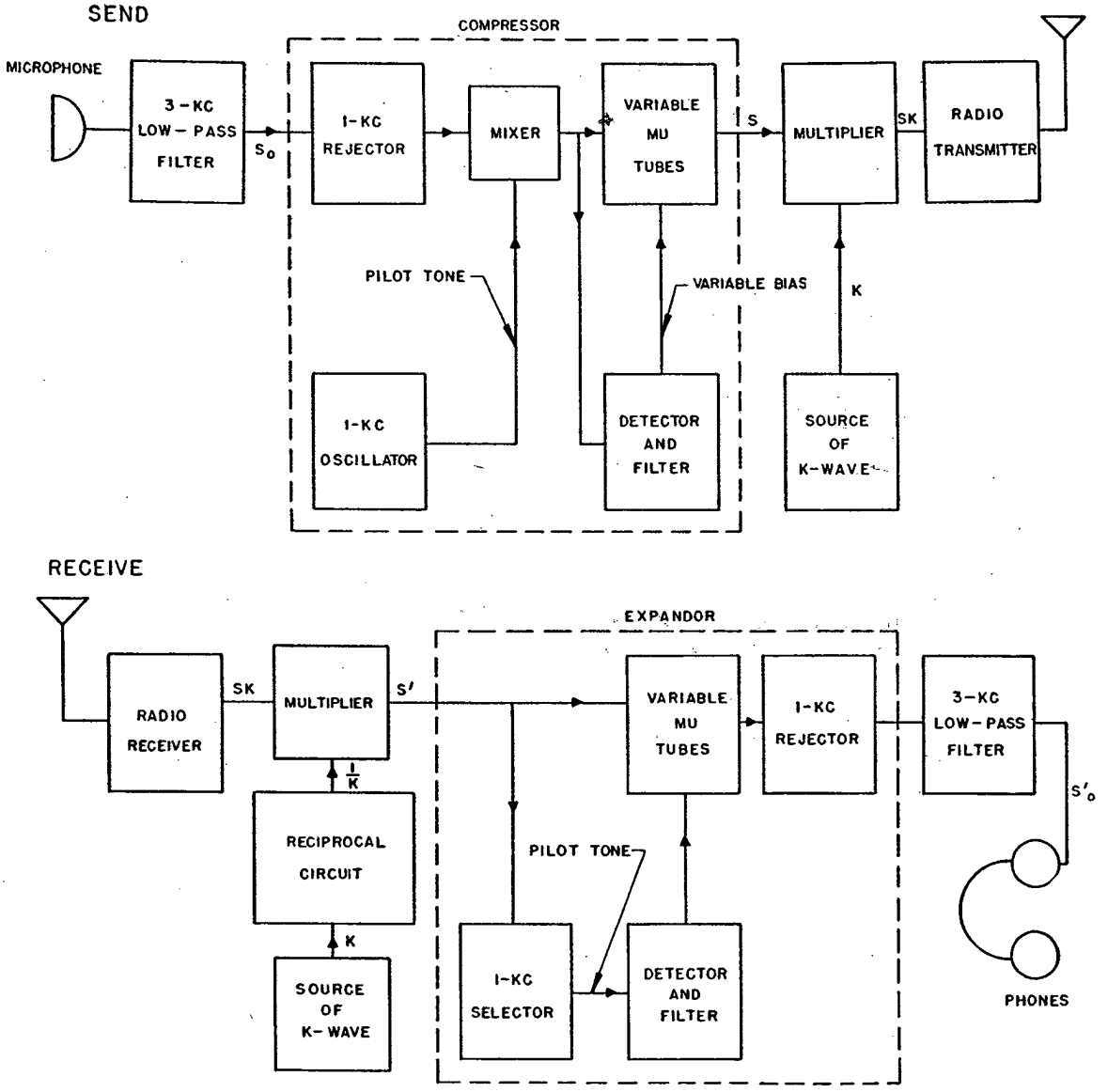



FIGURE 2. Block diagram showing compandor in RCA-Bedford privacy system.

3.1.3

## Compandor

The name "compandor" is derived from the words "compress" and "expand." It is an old device designed to improve the signal-to-noise ratio in communication by raising the level of transmission of the weaker sections of the speech signal with respect to the strong sections of the signal. This is equivalent to compressing the higher sections. At the receiving end the various sections of the signal are restored to their original relative levels.

In the present case the compandor is used, primarily, to destroy the cadence (or loudness variation) of the coded signal, and thereby improve the security. To further this end, a special compandor circuit was developed, in which a pilot tone is used to fill the space between words, and to provide control for the expanding process at the receiver.

The curve $S_0$ in Figure 3 represents the amplitude, or envelope, of a word of speech. This is fed into the compressor (i.e., the sending part of the compandor) as shown in Figure 2. A filter removes any 1,000-cycle speech components, and then the output of a 1,000-cycle oscillator is added in the mixer. This gives the combined envelope shown as "$S_0$ + tone" in Figure 3. The amplitude of the tone is about 10 per cent of that of the loudest section of the speech. The output of the mixer is detected, filtered to remove the audio frequencies, and then used to vary the bias of a pair of push-pull variable-mu tubes which amplify the mixed signal. This bias control is such as to make the combined signal $S$ have a substantially constant loudness as shown at $S$ in Figure 3. Note that the lower speech levels are raised. This signal contains a variable amplitude of 1,000-cycle tone, as shown at $T$. The signal $S$ is then coded by multiplying by the code wave $K$, and transmitted.

At the receiver, as shown in Figure 2, the received signal $SK$ is decoded to $S'$. In the expander, the 1,000-cycle tone is selected by a filter, and then detected to control the gain of a pair of variable-mu tubes. The variation in gain is such as to restore the amplitude of the tone component of the output to a constant value, and simultaneously restore the speech level to its original proportions. A filter then removes the control tone, and a 3,000-cycle low-pass filter removes the high-frequency distortion components from the phone circuit.

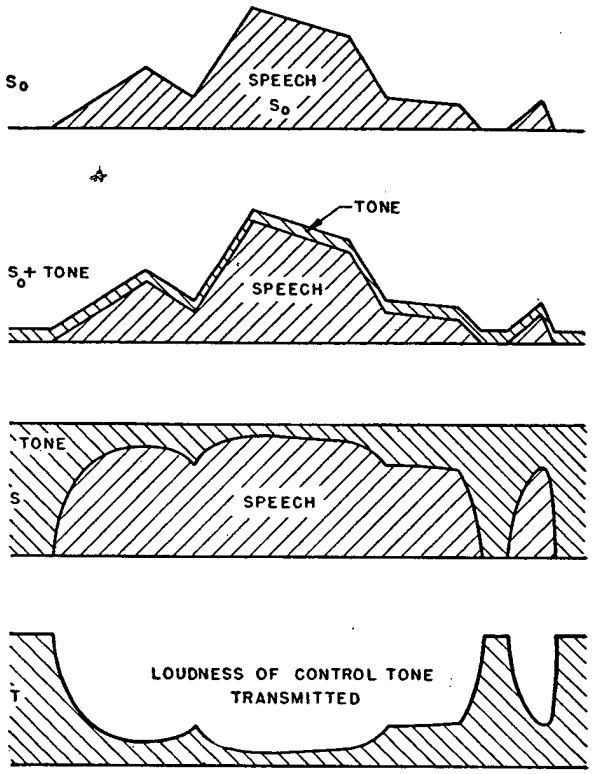



FIGURE 3. Envelopes of speech and tone in compandor.

When the signal transmitted in this manner is received on a privacy unit, operating with a code wave that differs substantially from the code wave at the sending end, the pilot (1,000-cycle) tone is spread irregularly over the audio spectrum so that a filter cannot isolate it for operating the expander to restore cadence. Neither can a filter be used to remove it from the phone circuit. The result is an unintelligible mass of coded speech and noise. Tests show that to get intelligibility from the decoded signal, the sending code wave and the receiving code wave must have a higher degree of similarity than when the compandor is not used.

Inspection of Figure 2 shows that most of the parts of the privacy unit, used in sending, are the same as used in receiving. Therefore, in a send-receive unit, the use of suitable switches or a relay avoids duplicating these parts.

### 3.1.4 Generating Code Wave by Delay Network

The coding wave $K$ in the system is generated by combining with different changeable polarities the outputs from taps along a delay network which is fed with narrow pulses from a fixed-frequency multivibrator, illustrated in Figure 4. The network contains 80 sections of series inductance and shunt capacitance. A repeater and an equalizer (not shown in the figure) are inserted at 16-section intervals to make up for attenuation along the network.

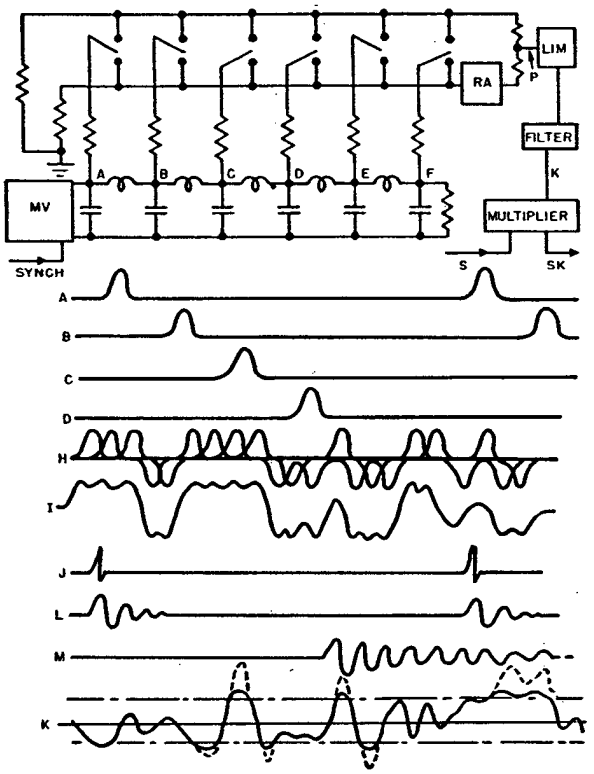



FIGURE 4. Generation of coding wave $K$.

The multivibrator [MV] supplies repeating pulses to the input $A$ of the delay network, as shown by wave $A$ in the figure. The frequency of wave $A$ is such that immediately after a pulse has reached the far end of the network, another pulse is fed into the near end. Then, neglecting distortion for the present, the voltages at tap points $B$, $C$, $D$, etc., are like $A$ except delayed various amounts in time, as shown.

Each tap is shown here with a SPDT switch so that it can be connected through suitable buffer resistors to point $P$, either directly or through a polarity-reversing amplifier [RA]. (Actually, the switching arrangements are more complicated than shown here, as will be explained, but Figure 4 suffices for an elementary explanation.) The voltage at point $P$, therefore, consists of the sums of the various voltages along the network taken either positively or negatively, depending upon the switch positions. Wave $H$ illustrates various pulses which would combine to form a wave such as $I$, which has a variety of widths of lobes. From this simple illustration, it is clear that a variety of complex waves, having a repetition rate of 100 times per second, could be produced by various switch settings.

Actually, the multivibrator tends to produce a very narrow repeating pulse, as shown at $J$, instead of a smooth, wide pulse, as shown at $A$. However, the multivibrator shock excites the first section of the network, resulting in an oscillatory voltage wave, as shown at $L$, to occur at tap $A$. As the pulse progresses along the network, the phase distortion of the network (which is very pronounced shortly below cutoff frequency) causes the pulse to have an extended oscillatory "tail" as shown by wave $M$. The voltage at point $P$ then is the sum of many waves which are, themselves, quite complex in shape, and may have lobes with a large variety of amplitude, as well as widths as shown at $K$ in the figure.

In this privacy system, the instantaneous voltage of the transmitted signal $SK$ is proportional to the instantaneous value of wave $K$. Then, if the coding wave $K$ were allowed to have peak amplitudes far in excess of its average amplitude, the average utilization of the available transmitter power would be very low.

Accordingly, to improve the power efficiency of speech transmission, the high peaks of wave $K$ of Figure 4 are limited to amplitudes considerably lower than the original amplitudes, shown by the dotted peaks. The limiting action is gradual in order to retain some amplitude variation in the code wave. After the limiter, a small shunt capacitor serves to smooth over the discontinuities in the wave caused by limiting.

### 3.1.5 Synchronization of the Delay Network

Consideration of the decoding process shows that it is necessary for the receiving code wave $K$ to have the same timing as the code wave at the sending apparatus (after making suitable allowances for the time of transmission of the signal). To maintain this condition, a synchronizing pulse is transmitted along with the signal $SK$, to control the multivibrator pulsing the network of Figure 4 when receiving.

Briefly the coded speech signal is interrupted for about 0.001 sec each 0.01 sec and a synchronizing pulse is inserted. At the receiver this pulse is selected by virtue of the regularity of its occurrence (as compared to any lobe of the coded speech) and used to trigger the receiving multivibrator which pulses the delay network which, in turn, generates the code wave.

### 3.1.6 Code-Changing Method

The eight code disks which are part of a rotary code-changing switch may be seen in the

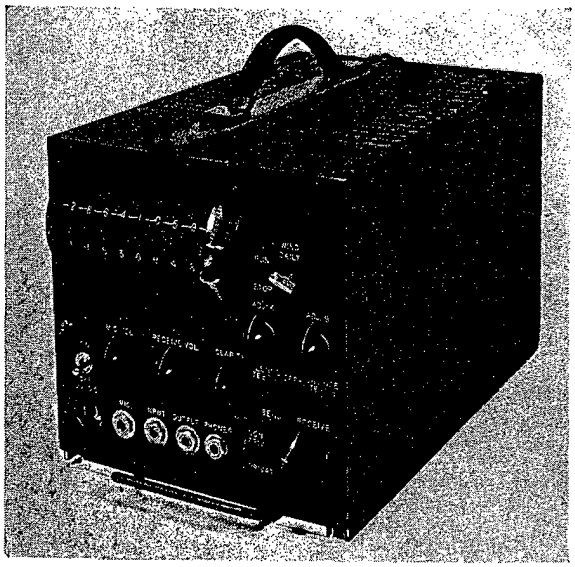


FIGURE 5. Front view of Model RCAL-1 privacy equipment.

photograph of Figure 5. Each code disk has twenty insulated silver segments, of three different types, which are located in irregular order in a circle
of three brushes
code disk so that
SPDT switch whi
tive depending u
under the brush. E
controls two taps o
two buffer resistors
between the 80 dif
forty switches is irr

The eight code disk
on a drum by eight
each disk can be set
twenty possible positions. The
the disks is rotatable by revolution
solenoid in steps of 1/100 intervals by
enoid is energized at 3-sec intervals by
controlled by a spring-driven clock. A
fixed to the right-hand end of the drum
brated in 100 equal divisions.

### 3.1.7 Auxiliary Compandor and Equalizer Unit

In the coding process used in Model RCA
each original speech frequency component
shifted both upward and downward in
quency by each frequency component of
code wave. This method diffuses the frequ
components of the speech quite thoroughly
Therefore, it is believed that most of the in
ligibility obtained by listening to the cod
wave $SK$ is due to the cadence of the words.
destroy the cadence of the speech to be scra
bled and therefore to improve the security,
special compandor described briefly in the be
ginning of this summary was developed.

### 3.1.8 Weakness of Short Repeating Code Waves

In Figure 6, a code wave $K$ is shown multiplied by a section of speech wave $S_a$ to form the coded wave $S_aK$. The coded wave crosses the axis each time the code wave crosses its axis, and also when $S_a$ crosses its axis. Similarly, a different section of speech wave $S_b$, when multiplied by the *same* section of code wave $K$, results in coded wave $S_bK$. In this wave, those crossovers produced by $K$ correspond in time

with crossovers in wave $S_aK$, but other crossovers do not agree.

At $SK$ are superimposed several sections of speech wave coded by identical sections of code wave, such as would occur with the repeating code wave of Model RCAL-1. This is substantially the image seen in an oscilloscope picture of the coded signal when properly synchronized by the transmitted synchronizing pulses. Inspection of this image readily reveals the probable location of the crossovers of the code wave, and also indicates the shape of the coding wave. This is particularly true if a large number of waves are superimposed, as seen on an oscilloscope with a long-retentivity screen. It has been demonstrated that a rectangular wave, as shown at $K'$, can be used effectively to decode a message transmitted by the code wave $K$. Hence, it is only necessary to determine, and make suitable use of, the location of the crossovers of the code wave to crack the message.

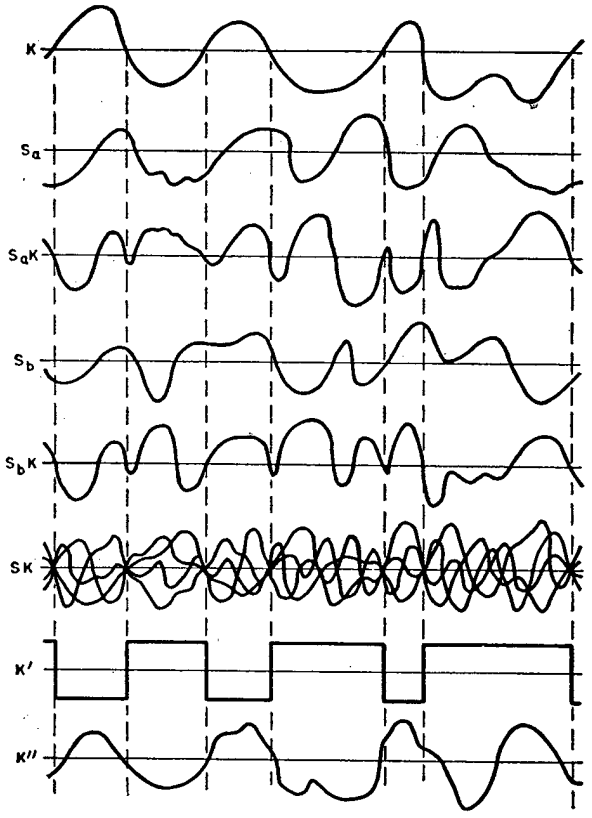



FIGURE 6. Wave forms demonstrating weakness of short repeating code wave.

The code wave of Model RCAL-1 has (by count), on the average, about 25 crossovers which repeat at intervals of 0.01 sec. The crossovers are spaced at irregular intervals, depending upon the settings of the code switches. The wave is composed of the various harmonics of the 100-cycle fundamental from about 300 to 2,500 cycles per second. The harmonics have various phases and amplitudes. This code wave is changed, in part, each 1½ sec through a 5-min cycle by the clock-driven rotary switch which contains the eight code disks mentioned above. Ten of these small partial changes, occurring in 15 sec, may cause a complete change of all contacts. Therefore, only sections of about 5 sec of the message would be cracked by a single code wave.

Although considerable apparatus of a very special character would be needed to actually crack a message coded with such a repeating code wave by making use of the repeating pattern of crossovers in the coded wave, as determined by statistical observation, nevertheless it must be appreciated that a suitable accurately calibrated oscilloscope could be used to observe the coded wave and determine the timing of the crossovers of the code wave, and that a suitable special apparatus could then be adjusted to produce a decoding wave such as $K'$ of Figure 6 to crack the message. Furthermore, there is a feasible plan for an apparatus to do the entire job automatically. Hence, no coding wave which repeats in a reasonable time can provide a high degree of security against an able enemy.

For the sake of completeness of this discussion, it should be pointed out that a message coded by a code wave such as $K$, in Figure 6, can be decoded by using a receiving code wave, such as $K''$, which differs considerably from $K$. From observation, it is estimated that if most of the crossovers of the receiving code wave occur within 20 or 30 per cent of the time of occurrence of the crossovers of the sending code wave, the message can be cracked even when the compandor is used. (The per cent value used here is based upon the intervals between adjacent crossovers in the sending code wave being 100 per cent.) Also, a few extra crossovers in either code wave, having no corresponding crossovers in the other wave, may be tolerated. With such a wide tolerance in the

cracking code wave, it is not surprising that in Model RCAL-1, which uses a repeating code wave having an average of only 25 crossovers, a short message can be cracked in a short time by "playing" with the code disks, or switches, at random.

Since all limitations of security of Model RCAL-1 with the compandor arise directly, or indirectly, from the repetitive character of the coding wave, the use of a nonrepeating code wave would appear desirable.

### 3.1.9 Dual Delay Networks for Generating Long Code Wave

In a system providing longer security, the period of the code wave could be made 0.4 sec (as compared to 0.01 sec) by using two delay networks operating at slightly different pulse frequencies to generate the code wave. This is a purely electrical device. Then the mechanical apparatus for changing taps on the networks can operate at the relatively low speed which causes a substantially complete change in each 0.4-sec interval, and thereby prevent the code wave from repeating itself until the mechanical system has run through its complete cycle. The time for this is over an hour.

The dual delay network appears to be a very economical electrical device for generating a code wave with a period as long as 0.4 sec. To generate a wave of this period and maximum frequency directly by a single delay network, would require about 3,000 LC sections.

### 3.1.10 Motor-Driven Tap Switch with One-Hour Period

In the dual delay system, it is required that a critical number of taps on the dual delay networks be changed each 0.4 sec to prevent a repetition of the code wave 2.5 times a second, which would allow a statistical study of the coded wave $SK$ to reveal information as to the location of crossovers in the code wave $K$. This is accomplished by a three-speed motor-driven rotary switch.

The switch, designed for the proposed long-security system has nine code disks and brush holders instead of the eight in Model RCAL-1. The 45 SPDT switches provided are connected in irregular order to control the 84 taps in the dual delay networks. These nine code disks are rotatably mounted with individual detents in groups of three on three separate drums. The three drums are geared to run at slightly different speeds, which are, respectively:

$$S_1 = 6 \text{ rpm},$$
$$S_2 = 6 \times \frac{20}{21} = 5.71 \text{ rpm},$$
$$S_3 = 6 \times \frac{20}{19} = 6.31 \text{ rpm}.$$

To the left of each group of code disks is a timing disk which is fixed to the drum so that it controls all three code disks in its group. Each of three 40-tooth gears is rotatably mounted on a counter shaft, but is restrained from relative rotation by an eight-position detent. These three detents allow the three timing disks to be independently adjusted to their proper starting positions by hand. The timing disks are calibrated, and numbered in 20, 21, and 19 equal divisions, respectively, to agree with the detent positions on the counter shaft acting through the three different gear ratios. All code disks have twenty positions on the drums, indicated by letters.

The speeds of the three groups of code disks are such that the system requires about 1 hr 6 min to run through a complete cycle, so that all groups reach their starting position simultaneously. Therefore, by resetting the individual code disks to a new code each hour, a nonrepeating code wave is provided. Any *two* groups of the disks go through a cycle in about 3 min. Then, if the effect of the other group of three disks upon the code wave were sufficiently small, the code wave would effectively repeat about twenty times each hour, and become accessible to the enemy.

Tests, however, made with Model RCAL-1, operating with the compandor and with a temporary motor-drive for the disks, showed that with three of the eight disks off code only 6 per cent of words were understood. (Each word was repeated three times.) With two of eight disks "off," 25 per cent were correctly understood.

To keep the motor in the receiving apparatus in synchronization with the motor at the sending station, both synchronous motors are driven by 60-cycle power whose frequency is controlled by a 145-kc crystal.

### 3.1.11 Probable Security of the System

Based on tests made on the Model RCAL-1 with compandor and a temporary motor-drive, it is concluded that, to obtain from a captured machine adequate intelligibility to crack a message, the enemy would have to have at least six of the nine code disks in the correct position. The probability of this condition being obtained in a single trial, at random, is 1/889,000.

It is estimated that at least 3 sec would be needed to set up and try each of the many possible code disk positions, even if elaborate special means were built to allow orderly adjustment of the relative positions of the disks while running. (The time for trying *each* code setting is made longer because of having to make a short exploration for correct phase of the entire disk assembly.) Hence, the *average* time for reaching the condition for six code disks right is:

$$\text{Time} = \frac{3 \times 889{,}000}{2 \times 60 \times 60} = 370 \text{ hr.}$$

(The use of more cracking setups would shorten this time.)

If this time is deemed inadequate to provide the desired security, it could be greatly extended by adding a few more code disks. An alternative method would use a selector switch of the radio-band-selector type for manually changing the connections between the motor-driven switch and the taps on the delay network. The setting of this switch would be part of the code.

No reasonable method of cracking messages sent by this system, other than the trial method above, occurred to the RCA engineers. Bell Laboratories' engineers (Project C-43) and others were given complete verbal descriptions of the proposed system, and invited to find some property of the coded wave by which it might be decoded. No likely property was revealed.[27] Of course, it cannot be known with certainty that the signal could not be cracked eventually by a shorter method.

By contrast, the basic weakness of the Model RCAL-1, with its repeating code wave, was known and reported very early, that is, well before design was begun. The clock-driven code switch was included with the expectation that it would only make cracking a more laborious process. (After the model was built, it was found that a message could be cracked by "playing" with the code disks somewhat quicker than originally expected. This was because it had not been appreciated how different the receiving code wave could be from the sending code wave and still give appreciable intelligibility.)

In studying the probable security of the proposed system, it should be remembered that the signal $S$ (which is coded to form $SK$) usually contains a very substantial amount of the 1,000-cycle compandor control tone. Offhand, this fact would seem to offer the most likely approach to a reasonable method of cracking. If this were found to be so, it would be necessary to use some other apparatus to replace the compandor. Two different devices are available but they are not attractive.

### 3.1.12 Present Status of the Development

Part I of the final report[14] of the project gives an assessment of the speech quality transmitted by the system and indicates that radio transmitters and receivers somewhat better than actually used during the war would be required to deliver good intelligibility. Weights and dimensions are to be found in the final report.

At the close of the project most of the new circuits required in the proposed high-security system had been developed. Some of these developed and used in Model RCAL-1 are: the wave multiplier, the reciprocal circuit, delay network and tap switching circuits, synchronizing circuits, synchronizing blanking circuits, and the compandor.

The following additional circuits were developed, or tested specifically to be used in the proposed high-security units: the "clip, multiply, and phase-distort" method for blending the

outputs of two delay networks was tested and shown to produce a coding wave with *more* crossovers and with the initial crossovers adequately "smeared." A synchronous motor suitable for driving the code disks had been driven by an amplifier from a chain of frequency-dividing multivibrators.

The rotary code switch had been designed, but not detailed. It included code disks, brushes, brush holders, and detents, which are very similar to parts in Model RCAL-1.

### 3.1.13 Conclusion

It was concluded that the speech privacy unit proposed would probably have a relatively high degree of security, that it would have dimensions and power requirements which allow it to be portable, and that it could be developed with reasonable expenditure of time and money.

## 3.2 HAZELTINE BAND DISPLACEMENT SYSTEM

The Hazeltine speech secrecy system[b] is of the band displacement type in which the speech is inverted and displaced in frequency to seven successive positions in an extended a-f band, in a sequence determined by a coding switch and punched cards.

### 3.2.1 General Description of the System

In transmitting, speech is first passed through a frequency selective network in which the frequency spectrum is tipped up at the rate of 6 db per octave. It is then modulated with a 13-kc carrier and the upper sideband extending from 13 to 16 kc selected in a band-pass filter. This is again modulated by a selected sequence of seven displacement carriers, 1 kc apart from 17 to 23 kc. The lower sideband is then selected, resulting in inverted speech in a sequence of bands in a range from 1-4 to 7-10 kc. Amplifiers are employed in the carrier channel to maintain the output at the same level as the input.

In receiving, the same apparatus is used. The speech is passed through the system in the reverse direction for unscrambling and at the normal speech end of the channel the frequency spectrum is tipped down by 6 db per octave to restore the original frequency characteristic.

An electronic switch for keying on the 17- to 23-kc displacement carriers for 50-msec intervals in a selected sequence comprises a chain of seven switching tubes. Each of these is arranged to generate a 50-msec pulse. The termination of this pulse initiates operation of the succeeding switching tube. In transmitting, the pulse from the last of the switching tubes is returned to the first to make the operation continuous. The pulses derived from the switching tubes are delivered to the seven carrier frequency oscillators as selected by the coding switch and serve to key-on the oscillators.

To synchronize the receiver and the transmitter, the pulse derived from the last of the switching tubes in transmitting is suitably amplified, limited, and filtered to eliminate components above 1 kc and then added to the scrambled speech at the end of the carrier channel. In receiving, this synchronizing pulse is separated from the scrambled speech and, after amplification and limiting, is applied to the first of the switching tubes. The connection between the last switching tube and the first is eliminated in the receiver so that operation of the electronic switch in receiving is initiated by received synchronizing pulses only.

To reduce the possibility of actuation of the electronic switch by spurious pulses, a barrier circuit in the form of a pulse generator having slightly less than a 350-msec period, is placed ahead of the first switching tube. Once a synchronizing pulse actuates the barrier circuit (and simultaneously the first switching tube) the barrier circuit becomes immune to further pulses during its cycle. This prevents any pulses from reaching the first switching tube until almost the entire cycle of the seven switching tubes has been completed.

### 3.2.2 Performance of First Two Models

Two models embodying such a system were completed, tested, and demonstrated to members of Division 13. Although it was possible to obtain speech of reasonably understandable

[b] Project C-15, Contract No. NDCrc-139, Hazeltine Corporation.

quality after a complete cycle of scrambling and unscrambling, it was felt that the performance could be appreciably improved in several ways.

It was felt desirable to reduce the degradation of speech quality obtained with the equipment. This degradation was probably caused by the following factors. The oscillators did not respond immediately to the keying pulses so that intervals of several milliseconds were left at the transition points for the displacement carriers. This resulted in blanks in the speech and in transient clicks. The frequency stability of the oscillators was poor with the result that synchronization between oscillators in the transmitter and those in the receiver could not be held. This resulted in slight changes in pitch of the speech as the displacement carrier frequency changed. There was also some nonlinearity present in some of the amplifiers.

It was also found that when as little as 10 db attenuation was inserted in the line between the transmitter and the receiver, the receiver had a tendency to drop out of synchronization with the transmitter. It was felt that the equipment should be designed to tolerate an attenuation of at least 25 db below the normal level. No experience had been obtained on the effect of noise and code interference on the synchronization of the two units. It was felt that reasonable immunity to such interference was an important requirement of the equipment.

### 3.2.3 Construction of Third Model

With the experience gained in the operation of the first two models, the construction of a third model was undertaken. The objectives sought in this third model were as follows:

1. Improved oscillator frequency stability.
2. Fast keying on and off of oscillator.
3. Elimination of nonlinearity in amplifiers in the carrier channel.
4. Substantially flat overall frequency characteristic from 300 to 3,000 cycles per second.
5. Improved immunity to changes of level and noise in the synchronization of the receiver.
6. Incorporation of a storage battery operated power supply.
7. Improved isolation and shielding of components to avoid carrier leakages and cross modulation.
8. Incorporation of a code switch suitable for operation with a punched card.
9. Closer approximation to a production design.

The third model, completed in the latter part of September 1941, met the above objectives very well. Speech quality was materially improved over that obtained with earlier models. Switching transients between successive displacement carriers could not be detected in the output. The prominence of the sync pulse in the output was greatly reduced. Measurements indicated that the distortion of the system was reasonably low. The input to the receiver could be reduced more than 25 db below normal level before the receiver dropped out of synchronism. With high noise levels the receiver remained in synchronism at least up to the point where the noise was equal to the signal.

### 3.2.4 Apparatus Details

The final report[15] on the project gives details of the transmitting and receiving circuits, means for providing nonscrambled speech when desired, method of setting up the desired code by means of punched code cards, an analysis of the inherent secrecy of the system plus the chances of cracking it, and suggested improvements.

The equipment weighed 45 lb, required approximately 1.14 cu ft of space, operated from 6.3 volts and needed 10 amp at this voltage.

# Chapter 4

# UNSCRAMBLING AND DECODING METHODS

## 4.1 HISTORY

ALONG WITH PROJECTS and work primarily concerned with the development of scrambling methods for speech, code telegraph, or facsimile, projects concerned with unscrambling or code-cracking methods engaged a large part of the time and energy of those associated with this portion of Division 13 activity. In this manner the effectiveness of the privacy methods developed could be tested constantly.

Realizing early in the privacy research conducted under the sponsorship of Division 13 that the ear had very limited capabilities for analyzing scrambled speech, the sound spectrograph was developed by the Bell Telephone Laboratories to provide speech patterns which could be interpreted by the eye. In effect this valuable instrument divided scrambled speech into its three important dimensions of frequency, amplitude, and time. By its means, any alterations to the original speech in either frequency or time could be detected and analyzed with the object of adjusting unscrambling apparatus so that the original speech could be recovered.

Early in 1941 a rough laboratory model of the sound spectrograph was demonstrated to the National Defense Research Committee [NDRC] and as a result Project C-32 was organized with the immediate object of producing such a device in a form that would be useful for diagnosing and decoding speech scrambling systems. Such a model was produced and successfully demonstrated to representatives of NDRC, Army, and Navy.

Upon the termination of Project C-32 on February 1, 1942, it was decided that the work initiated under that project should be continued. Accordingly Project C-43, "Continuation of Decoding Speech Codes," was authorized. The project anticipated some routine decoding, the production of duplicate equipment to be used by the Army and Navy intelligence services, and further studies of decoding tools and methods. At that time the Army and Navy were relying almost entirely upon this project to furnish the above services until they could be provided with suitable equipment and could obtain trained personnel. Based on the needs of the military, this project was thrice extended.

Under the guidance of NDRC Division 13, the emphasis was placed at any given time on what was deemed to be most urgent. This is reflected in the subject matter of the preliminary reports of Project C-43 which were issued from time to time and which form the appendix to the final report of that project. In addition to the specific investigations covered by these preliminary reports much work was carried on as the basis for more general coverage of the field of interception, diagnosis, decoding, and evaluation of speech privacy systems.

In addition to the general studies mentioned above, decoding equipment was developed and models furnished to the Army and Navy. This decoding equipment included (1) two models of the sound spectograph, (2) a variable-area pattern machine, and (3) equipment for decoding two new enemy privacy systems intercepted by the project personnel at Point Reyes, California. In each case Army and Navy personnel were instructed in the operation and maintenance of these equipments.

Intercept activities of the Project C-43 personnel included (1) the study of recordings submitted early in the project by the Federal Communications Commission, (2) exploratory work at the Bell Telephone Laboratories experimental radio receiving station at Holmdel, New Jersey, and (3) exploratory work and routine interception of radio telephone transmissions at the American Telephone and Telegraph Co. radio receiving station at Point Reyes, California. Reports of the results of the above studies and recordings of intercepted material were submitted directly to the interested military authorities.

Many speech privacy schemes were submitted through NDRC during the course of this project. These were studied and evaluated. This

work led directly to the continued improvements of the sound spectrograph and the development of supplementary decoding tools and techniques.

As the Army and Navy became able to carry on decoding activities themselves with the aid of equipment and information furnished by NDRC as the result of work outlined above, the activity on Project C-43 gradually decreased. The final reports on the several projects cover all phases of the work on the general subject and constitute a reference work for future studies of speech privacy systems.

In this chapter will be found, first, some general observations on the intercept problem and on methods of cracking scrambled speech, a general description of the sound spectrograph and examples of its applications, and some material on the practical evaluation of privacy systems, all taken from the final report on Project C-43.[1] Then follows a summary of the work accomplished in the several decoding projects working under Division 13 sponsorship.

## 4.2 INTERCEPTION

Speech privacy systems may be used in connection with radio telephone systems or with wire systems. The unauthorized interception of wire communications in wartime, however, was beyond the scope of the work done for Division 13. These notes therefore are confined to radio interception problems and expands the material in Preliminary Report No. 25.[45] The decoding techniques to be described subsequently, of course, apply to wire as well as radio communications.

### Types of Radio Systems

Radio telephone systems range in size and complexity from high-power point-to-point stations operating over great distances to the low-power, short-range sets carried by individual soldiers. The high-power systems are usually designed to operate between specific points, using specific assigned frequencies. They are equipped with elaborate fixed antennas, which are usually of the directive type. Privacy equipment associated with such terminals may be as large and complex as desired to achieve virtual secrecy. A major consideration in such systems, of course, which adds to size and complexity, is that the privacy must not degrade the quality of the received speech to any appreciable extent.

On the other hand, anyone can intercept these high-power signals at great distances, where he can have a well-equipped centralized decoding laboratory, with no limitation on the size and complexity of the decoding equipment he might bring to bear. This laboratory can be adequately manned by a relatively few highly trained decoding specialists not necessarily members of the Armed Services.

In contrast with this situation, the low-power, short-range radio sets used in military operations are severely restricted as to size and weight, and these restrictions also apply to privacy equipment. The smallest privacy set submitted to Project C-43 for study was roughly a 10-in. cube, and was designed for mobile applications like tanks, planes, and command cars. While it is difficult to achieve a high degree of inherent privacy in mobile equipment, it should be noted that the very mobility of such systems adds to the security, because the signals can not generally be picked up at great distances, and whatever equipment an intercepter might use to crack the privacy must also be mobile. Furthermore, the decoding equipment must be operated by military personnel, a large number of whom may be required if the enemy is making extensive use of mobile privacy.

Intermediate types of radio systems are used for the higher echelons of command. For such applications, the radio equipment is semimobile. It can be transported in trucks and set up very rapidly, and may have a considerable range. For such applications, a high degree of privacy is required, and a truckload of equipment might be justified, because the enemy could afford to devote considerable time, personnel, and equipment to decoding the kind of messages which would be transmitted over such systems.

### Intercepted Signal Quality

Since most of this chapter deals with decoding, the material from this point on will be written from the point of view of the unauthorized rather than the authorized listener. It is first of all desirable to get a good signal, as

free as possible from interference. There are several reasons for this. First, the process which unscrambles the speech also scrambles any noise such as static which has been superposed on the scrambled signal. This changes the time or frequency distribution of the noise, breaks up harmonic relationships, etc., thereby increasing the interfering effect of the noise. Second, the decoding is apt to be less perfectly accomplished than at the authorized terminals, which tends to make the speech harder to understand. Finally, there are usually language differences which still further add to the difficulty of understanding the message. Conversations can be carried on under extremely unfavorable conditions by people speaking their own language, but noise and poor quality rapidly degrade the intelligibility of a language foreign to the listener.

In this connection it might be noted that it is very desirable to be able to hear both sides of the conversation without interruptions, in order to follow the context. In the case of the point-to-point systems, this will in general require two receivers because the two directions are transmitted over separate channels at different frequencies. If the two outputs are mixed for listening or recording, however, it should be kept in mind that the noise on the weaker signal will be superposed on the stronger signal and may seriously degrade it. Putting the two signals on two headphones will improve this situation, because noise in one ear does not seriously affect the intelligibility of a signal in the other ear. This problem does not arise in the case of the smaller radio systems, because these are generally operated on the basis of switching between transmitting and receiving conditions on the same carrier frequency.

Methods of obtaining a good signal are the same for the interceptor as for the intended receiver. A few of the important considerations are listed here; further information on any or all of them can be had from radio reference works. (1) Point-to-point systems usually employ directive antennas; the intercept station should therefore be located along or near the line of the radio beam. (2) In locating stations to intercept radio transmissions in the h-f range, account should be taken of the skip distances of the frequencies involved. Better signals will sometimes be obtained by moving farther away from the transmitter rather than closer. (3) The use of directive antennas, directed towards the transmitter being monitored, will improve the signal-to-noise ratio by discriminating against noise which is nondirectional. These antennas of course should be designed for the frequency and polarization of the signal, and properly coupled to the receiving set. (4) Stronger radio signals will be received if the antennas are located in the open, with no trees or other obstructions in the foreground. This is particularly important in the v-h-f range. (5) Radio signals increase in intensity as the height of the antenna above the immediate foreground is increased, particularly for v-h-f transmission. Thus better results are obtained with the antennas located on high masts or on hills overlooking the foreground in the direction from which the signal is arriving. If the signal is in the v-h-f range and other measures are inadequate, it may even be desirable to consider receiving the signal in an airplane and recording it or retransmitting it for decoding. (6) Noise improvement can generally be obtained by keeping the receiving equipment away from sources of man-made noise, such as ignition systems and power lines.

### Receiving Sets

With regard to the receiving sets, a distinction must be made between the various activities of an intercept station. One important activity is searching for possible enemy transmission channels. The object is to determine all the channels in use, the location of their terminals, the type of business transacted, and, most of all, whether any special form of privacy is used on the channel. Some preliminary searches of this type are described in Preliminary Reports No. 2[46] and 23.[47] If no privacy is used, other than the usual commercial types, it is unlikely that information of military importance is transmitted over the channel, and it may not be necessary to monitor it continuously. If a new privacy system is located, however, it is very likely to be worth monitoring and decoding continuously.

For the searching and scanning activities, the

ordinary commercial sets of the "communications" type, equipped with a beat-frequency oscillator, will serve very well for all types of transmission. Even the suppressed carrier type can be handled very well provided the signal is fairly strong. It may require continual manual adjustment of the local oscillator, but sufficiently good reception can be obtained to determine the nature of the channel. Cases of extreme spread-band transmission can also be handled in this manner.

If a particular channel employing suppressed carrier is determined to be worth monitoring continuously, then a single-sideband receiver will give improved reception. These receivers are equipped to amplify the partly suppressed carrier, or supply a new one with great stability, and they may provide as much as 15-db improvement in signal-to-noise ratio in some cases. They also permit selecting either the upper or the lower sideband of double-sideband systems, which may be of advantage in cases where interference occurs on one or the other sideband of such systems. However, these receivers are not suitable for searching.

### Types of Radio Transmission

A knowledge of the types of radio transmission which may be encountered is very important to the personnel of an intercept station. Experience has shown that without such knowledge, the nature of intercepted signals may be completely misinterpreted. It is possible to mistake certain normal types of transmission for new systems, or conversely to fail to recognize new systems which should be monitored at once.

*Double-Sideband.* The commonest type of transmission is the double-sideband type in which the carrier is transmitted along with the sidebands, which are usually about 3 kc in width, and are located immediately adjacent to the carrier. These are readily demodulated by the ordinary receiver. This is true even if the carrier is rapidly wobbled, provided the wobble does not cover too great a frequency range. Such wobbles are sometimes used in combination with simple inversion, to prevent reinverting with a locally supplied carrier at the edge of one sideband.

*Spread-Band.* In this system, some or all of the sidebands are displaced from the carrier. Demodulated signals of this type will cover an a-f range greater than 3 kc, usually as high as 6 kc. It is essential, therefore, that the receiver be capable of handling such a band. To obtain the intelligence, the signals must be further demodulated (B1 in Table 1, page 47).

*Suppressed Carrier.* In the ordinary transmissions described above, the carrier level is high compared to the speech sidebands. To avoid loading up the transmitter with carrier, and thereby permit radiating a higher sideband level, many channels operate on the "suppressed carrier" basis. In this system the carrier is either eliminated completely, or transmitted with greatly reduced level. To demodulate such signals properly, the weak carrier must first be greatly amplified, or a new one supplied locally. If this is not done the signals will demodulate themselves around whichever component in the sideband happens to be predominant, producing thoroughly scrambled speech which can thereafter not be restored. This condition can be recognized by its characteristic sound to the ear, together with wide syllabic fluctuations of the meter which ordinarily indicates the carrier level.

*Twin Channels.* With suppressed carrier systems, usually only one of the speech sidebands is transmitted. However, a second sideband, transmitting a second speech channel, is sometimes added, usually displaced from the carrier by about 3 kc, to avoid crosstalk between the channels. This is called "twin-channel" operation, and gives on demodulation an audio signal covering about 6 kc. The two channels must be separated and placed in their normal positions by the methods cited under spread-band systems.

The above systems are the main types of radio transmission used commercially with amplitude modulation. In addition, in the v-h-f range and above, there are frequency-modulation systems, and also pulse-modulation systems, both of which require receivers specially designed to handle their particular types of signals. This is too large a subject to cover here, and reference must again be made to the radio literature.

Finally it should be mentioned that in addi-

tion to speech a great deal of telegraph transmission will be found. There are several types of telegraph signals, including hand-keyed, such as Morse code, or machine-keyed such as Boehme and teletype. Any of these types may be transmitted by keying the carrier, or by keying a tone modulated on the carrier. The marks and spaces may be represented by changing the amplitude (on-off) or by changing the frequency (two-tone). Finally, since telegraph requires a much smaller band than speech, it is often operated on a multichannel basis, that is, a voice channel will be divided into a number of telegraph channels. In addition, there are facsimile transmission systems, which also may be operated on an a-m or f-m basis. If a new signal is encountered whose nature is in doubt, these possibilities should be kept in mind for further investigation when the need arises.

### Recording

The same considerations which make it desirable to obtain a good intercepted signal, apply also to recording and reproducing scrambled speech. In addition to the requirements as to quality and noise, there is an even more serious one concerning speed regulation. In general, systems designed for a high degree of privacy require a high degree of synchronization, and in many cases ordinary recording methods are not good enough, not only in long-time average speed regulation, but also in the steadiness of the instantaneous speed. In the case of some of the systems the requirements are so severe that even the best commercial recorders will not meet them.

The best solution of this problem is to decode before recording. This will be possible in many cases, although it may sometimes entail the loss of parts of the message while adjustments are being made or the code is being determined. It happens that some systems which impose the severest requirements on speed regulation (B3 in Table 1), can be handled in this way. When this method is feasible, even poor quality recorders, such as those designed to record a great deal of material in a small area, may be good enough.

In some of the systems it will not be possible to decode before recording. It happens, however, that in the case of the only known system for which this is true (F3 in Table 1), the requirements as to quality and speed can easily be met by good commercial type recordings.

The matter of convenience or ease of use of the reproducing system is very important in decoding work. In this respect also, the requirements are different for different privacy systems. The recording systems using the embossing process, for instance, are convenient because they produce no thread, and they require little attention. However, they all suffer from poor tracking during reproduction, which can be exceedingly burdensome, especially where the material must be reproduced many times over. Recording magnetically on wire is attractive from the standpoint of convenience and also quality, but back-tracking is very time-consuming and laborious.

The best solution, at the present writing, appears to be disk recording on acetate, with a machine capable of recording at various speeds. Low speeds can be used where quality need not be too good, and a long record is desired. Higher speeds can be used where better quality is needed. Such recording systems are commercially available.

### Decoding Tools

In addition to the facilities discussed above, an intercept station, if it is to be prepared to diagnose and decode intercepted enemy signals, must be equipped with a considerable variety of special tools. These should include such well-known devices as oscilloscopes, amplifiers, oscillators, modulators, rectifiers, fixed and variable filters, and a supply of components for constructing special circuits that may be required. Some of the less well-known devices include magnetic tape or wire recording and reproducing equipment in the form of loops with multiple pickups, commutators for sweep or timing circuits, variable-speed drive mechanisms, channel shifters, the variable-area pattern machine, and the sound spectrograph. There should also be models of the more important types of existing speech privacy systems. Finally, and perhaps most important of all, there should be stationed at the intercept location a group of highly trained technicians, who should be thor-

oughly familiar with radio transmission problems, radio facilities, cryptanalytic procedures, and diagnosing and decoding methods. If these technicians are not conversant with the language encountered in intercepted communications, interpreters should be continuously available.

Even with all the special tools and personnel, decoding in many instances will be a difficult problem, and patience and painstaking effort will be required to obtain useful information from scrambled speech. Unless the needs have been anticipated the enemy may have secret communication for a considerable period of time as a direct result of unpreparedness.

## 4.3 NONCRYPTOGRAPHIC TOOLS AND METHODS

Beginners in the study of privacy systems never fail to be amazed at the difficulty of scrambling speech sufficiently to destroy the intelligence. The ear can tolerate or even ignore surprising amounts of noise, nonlinearity, frequency distortion, misplaced components, gaps, superpositions, and other forms of interference. Very often partial or even complete intelligence can be obtained from a privacy system by partial or imperfect decoding, and this in turn can often be accomplished by operating on the scramble in some way which the designer did not contemplate.

The fact that the ear is such a good decoding tool in combination with noncryptographic methods makes the production of privacy systems very difficult. Scrambling systems which look very effective on paper sometimes turn out on trial to degrade the intelligibility very little, although the scrambled speech usually sounds unpleasant. Most methods pushed to the point where they succeed in hiding the intelligibility so distort the speech that it is impossible to restore the speech with good quality. In fact, there are very few speech privacy systems which achieve a high degree of privacy with acceptable quality.

Noncryptographic methods are very important, because they may reduce the delay in obtaining the intelligence substantially to zero. Furthermore, they may render completely futile the most elaborately irregular code changing systems which could be handled only with the greatest difficulty by straight cryptographic methods. A number of noncryptographic methods are given below. Some of them, of course, result in poor quality, but the saving of time, labor, and equipment may be very great.

### CAPTURED SET OR FUNCTIONAL EQUIVALENT

With many privacy systems all that we need to listen in is a captured set or its functional equivalent built from knowledge of the scrambling method. An extreme example of this is simple inversion. In this case the scrambled speech is quite unintelligible to direct listening, but if we know it is inversion, we can find the inversion frequency very quickly by trial. Another example is the split-phase system (A5). The phase-shifting network in the captured set could readily be adjusted to demodulate either of the two overlapping sidebands.

Slightly more complicated systems are those with a simple program. Again with a captured set or its equivalent it is usually easy to find the program by trial. The only possible difficulty is in keeping step with the sending end, particularly if there is no synchronizing pulse. An example of this is a wobble band displacement (B3). If, for instance, the wobble is sinusoidal, with the frequency and the sweep limits known, the problem is to keep in synchronism. In this connection "aided tracking" might be mentioned, a device which is familiar in gunfire control circles. With this system changes in both frequency and phase are made simultaneously. This is illustrated in Figure 1. Suppose we

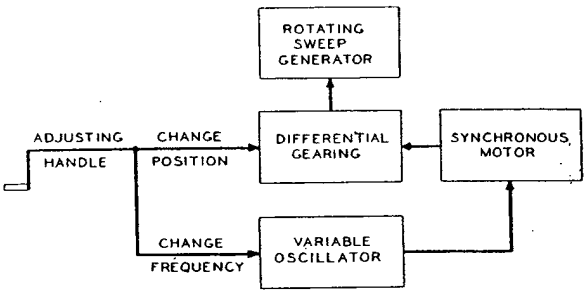



FIGURE 1. Method of aided tracking.

find ourselves slightly out of step with the signal. By rotating the adjusting handle forwards or backwards we can get back into step. Suppose this adjustment was in the forward direction. The fact that we had to catch up is an indication that the motor is slow. Therefore, some of the motion of the handle required for catching up is used by means of gearing to change the frequency driving the motor. The gear ratios are chosen to suit the particular problem. With this method it is possible to get into step with and stay in step with systems such as alternate displacements and regular wobbles.

### Compromise Decoding Methods

All the methods outlined in this section have been tried, at least in the laboratory. Their success, however, naturally depends to some extent on the switching rates and similar variables. It is possible, therefore, that a method might

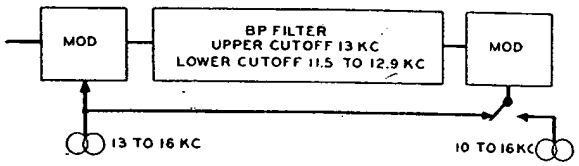



Figure 2. Band-shift filter; an important decoding tool.

prove unsuccessful against a scrambling system which seems to be in the same general class as the one that was tried in the laboratory.

Consider, for example, a system (A2) which involves inversion about a number of frequencies in succession. If these frequencies are not too far apart we can choose a single frequency somewhere in the middle range and demodulate the whole signal with this one frequency. The resulting band will be right side up, but displaced by varying amounts not exceeding half the total range. This has been found to be quite intelligible, provided the switching rate is not too high or the range of frequencies too wide.

With some systems it is expedient to listen to only a portion of the frequency range rather than the whole range. An outstanding example of this is the system in which the subbands are variously delayed (F1). Conceivably, these delays could constantly be changed with time according to a never repeating program. This, however, would be futile because with a band filter we need listen to only one of the bands, disregarding the others. Unless this band is very narrow the intelligibility may be practically complete. Similarly in band-splitting systems if the switching is not rapid (D1) we can follow one of the bands around the frequency range. The lowest or second lowest band is usually the best. Another example is the tone sequence (J3); instead of trying to filter out one tone at a time as it occurs, we can leave all the filters in all of the time and still have enough speech coming through to yield the intelligence.

A special case in which the rejection of a part of the frequency band of the scramble makes decoding easier concerns those systems such as A5 which depend on carrier phase to mix and then separate components. There is no phase requirement imposed on the demodulating carrier unless both sidebands are transmitted. Therefore, either sideband of such a system may be suppressed with a filter, and the remaining sideband demodulated with a carrier of any phase. The two signals in the sideband will then be simply superposed.

For purposes such as those outlined a valuable tool is the band-shift filter illustrated in Figure 2. With this device a band of adjustable width can be taken from any portion of the signal frequency range (0 to 3 kc) and relocated in any other portion of the same frequency range either straight or inverted. One form of band-shift filter is described in Preliminary Report No. 11 of Project C-43.[16] It consists essentially of a double modulator, but with a band filter of variable width. If the frequency location of the band is not to be changed, the switch in Figure 2 should be in the left-hand position. One form of variable band filter is shown in Figure 3. This tool has also proved useful in

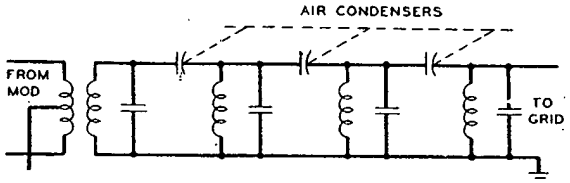



Figure 3. Band-pass filter in which pass band is variable.

certain other systems such as the multiplication system (H1) and the time division multiplex [TDM] system (E1).

Sometimes it is expedient to listen to a scramble only part of the time. Some of the simpler coding programs can sometimes be broken down in this manner by trial. For instance, if a coding cycle has $N$ elements we can listen to every $N$th element and make whatever adjustments are needed to make this sound natural. We can then listen to the next adjacent element and adjust the system so that these elements blend

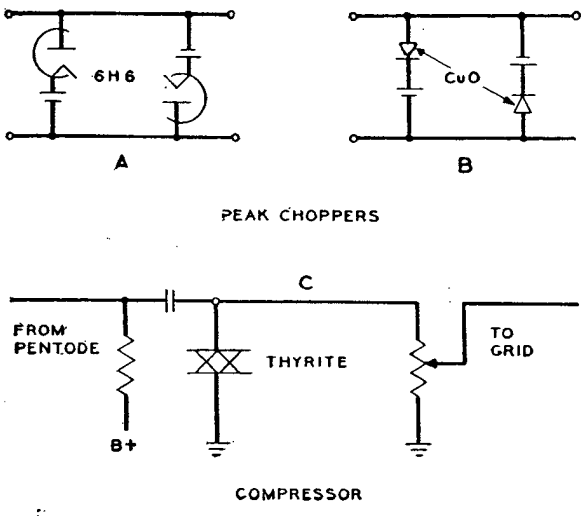



FIGURE 4. Elementary circuits of peak choppers and compressor.

properly. This attack applies to a system in which several different displacements are used (B2). A captured set, of course, is the easiest way of selecting every $N$th element because it is usually easy to make the other time elements inoperative.

Another useful device is the limiter, or peak chopper. In this same class is the compressor. These are illustrated in Figures 4A, B, C. They all tend to equalize the successive lobes of a complex wave. The peak chopper simply chops off any peak which exceeds a certain instantaneous voltage. The compressor operates more gradually and leaves the waves well rounded. If straight speech is put through any of these devices, distortion products are generated because the wave form is radically modified. It is found, however, that this kind of distortion damages the intelligibility very little. These devices should be useful against any privacy system in which sudden changes of level occur. A good example is the subband level modulation system (H3). A separate limiter or compressor in each of the subbands will tend to smooth out the level variations and make the speech intelligible.

Another nonlinear device is the rectifier. Two forms are shown in Figures 5A and B. The rectifier as used here should not be confused with the detector. The latter device also rectifies, but it then has a time constant incorporated in the output circuit which tends to smooth the output and give the envelope wave. The rectifying action which is wanted here simply takes all the negatives lobes of the signal and turns them over. As in the case of the limiter, straight speech put through a rectifier of this type is about 95 per cent intelligible.

In the privacy system designated A4 the phase of the speech signal is reversed at short irregular intervals. If this signal is now rectified, all the negative lobes will be made positive and the resulting wave will be indistinguishable from rectified straight speech except for slight discontinuities at the points where the reversals

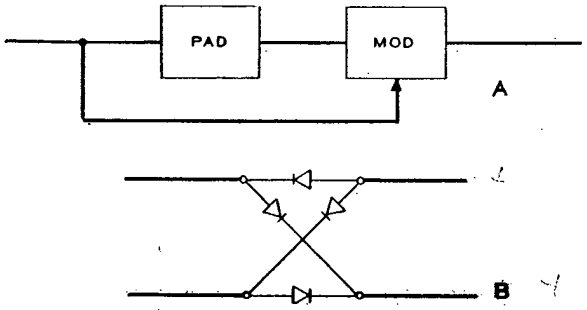



FIGURE 5. Two forms of rectifier circuits.

occurred in the privacy system. This is illustrated in Figure 6. Therefore, a simple phase-reversal system, no matter how irregular, should yield to rectification except that distortion in the transmission process tends to change the wave form and thereby degrade the quality of the resulting speech. It should be noted that the multiplication process (H1) also results in a phase reversal every time the coding wave passes through zero. It has been found that rectification tends to make this kind of scramble more intelligible also.

A very useful noncryptographic device is superposition. For instance, with a three-channel mixing system such as L1 or L2, if all three channels are listened to simultaneously, three conversations will be heard at once, or possibly one conversation with two noises superposed. Experience has shown that under such conditions it is usually easy to concentrate on the desired channel and ignore the others.

Another form of superposition is illustrated by the following: Consider a split-band system

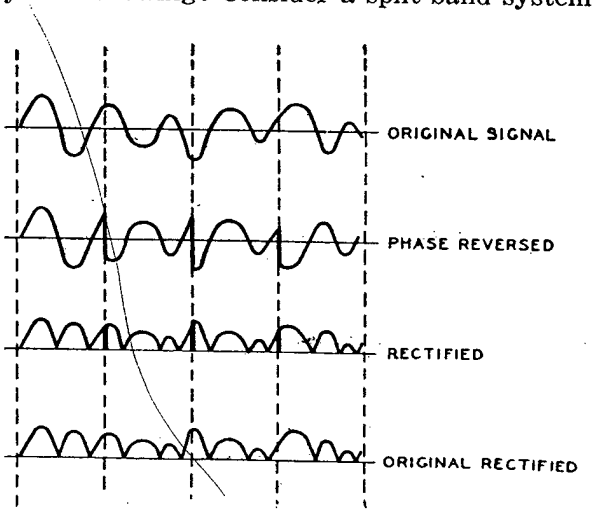



FIGURE 6. Action of rectifier, useful in breaking down multiplication scrambles.

(D2) in which six different codes are used in a never repeating sequence. This would be rather difficult to handle by cryptographic means. Suppose, however, we had six separate decoding units, each set to decode one of the six codes. If the scrambled signal were fed into all six of these decoders simultaneously, one of them would always have straight speech in its output. The other five would be scrambled. If these six outputs are all superposed, we will hear straight speech with five scrambled superposed. This straight speech can be understood quite easily. It will be noted that the unwanted components in this kind of superposition are derived from the wanted components, and always vary in level simultaneously with the wanted components; it appears that under these conditions they do not do much damage.

The split-band equipment illustrated in Figure 6 of Chapter 1 is adapted for this kind of superposition. A multiplicity of cross connections is made from each of the band-pass filters to the output modulators whereby each of the bands in the signal is placed in the desired bands in the output. Steps should be taken to see that these cross connections do not interfere with each other. An amplifier after each band filter, for instance, will perform this function. Figure 7 illustrates a simpler case of superposition applied to a system using two band shifts (B2).

It may be noted here that superposing time-displaced elements does not appear to be successful. For instance, if all the segments of the commutator in a time division scrambling [TDS] machine are connected to all the pole-pieces, the output will be straight speech with several scrambles superposed. This has been found to be completely unintelligible.

In certain cases which have been met in Project C-43 the privacy sets are equipped with dials or similar means which were intended to provide an easy method for obtaining a large number of different codes. In some cases the different codes may not be sufficiently different to be mutually private. That is, while there may be literally millions of different combinations, it sometimes happens that there are thousands

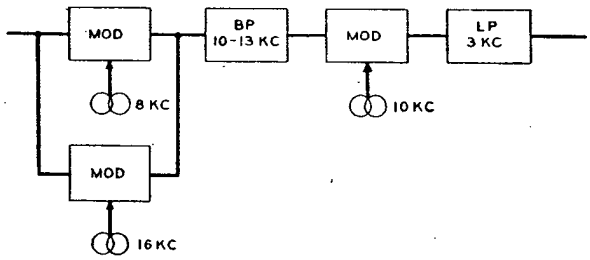



FIGURE 7. One form of superposition decoding.

of combinations which will decode material scrambled with one of the combinations. Various degrees of quality will result from these partial or incorrect decoding operations. However, as long as intelligibility can be extracted the codes cannot be considered mutually private. In such cases it is possible with a captured machine simply to manipulate the dials systematically or unsystematically and listen to the result. When the speech begins to sound somewhat natural, systematic trials of each dial in turn will sometimes steadily improve the quality. Something of this sort could be done

with simple TDS systems also, except that the use of interlaced codes makes this somewhat more difficult.

In certain cases where there are a large number of codes possible but only a few of these codes are good codes from the standpoint of direct listening, it would seem reasonable that any code applied to the scrambled signal should turn the good code into a poor code. In the five-band split-band system for instance, there are some 3,840 possible codes but only twelve or so are considered really good. Any code in

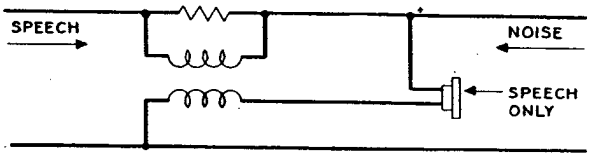



FIGURE 8. Use of directional discrimination against noise.

the decoding machine, therefore, should decrease the privacy for direct listening. This has been tried in the laboratory but has not been pushed to the point of determining whether it could compete with the superposition method. The idea may possibly apply to other systems which may be encountered.

A very specialized device, which applies to wire line communication only, should be mentioned here because it is not very well known. It distinguishes between the two directions of

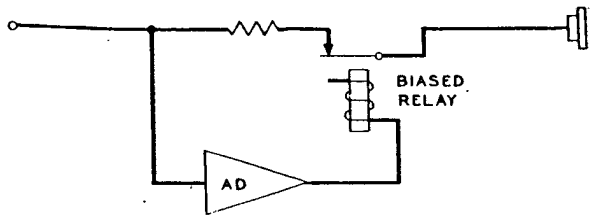



FIGURE 9. Use of relay to disconnect receiver from line during heavy bursts of noise.

transmission over wires. In the masking privacy system J2, for instance, the clear signal in one direction is masked by noise sent in the other direction. The device illustrated in Figure 8, however, discriminates against the noise, allowing the speech to be heard. It requires a small series resistance, which is built up by a step-up transformer to the line impedance. The secondary is connected to the other side of the line. The direction of discrimination depends on the phasing of the transformer windings.

### AUTOMATIC DECODING

Whether speech is intelligible or unintelligible is purely a subjective matter. However, the method of making speech unintelligible involves making physical changes in the speech wave. Certain kinds of physical changes can be detected quite readily by objective means and utilized to undo the scramble automatically. The most elaborately irregular code program is completely futile if this kind of decoding can be applied.

A very simple example of this is shown in Figure 9. Suppose the system consists of short spurts of noise applied in an irregular manner. The noise must be high in level compared to the speech in order to mask the speech. Therefore, if the signal is applied to an amplifier-detector, connected to a relay (or electronic switch) the relay can be so biased that it operates only on the noise spurts. The receiver is momentarily disconnected from the line whenever a noise spurt occurs. The same method can be used for level modulation systems (H2 and H3). Instead of disconnecting the receiver, the high-level portions of the signal cause the receiver to be connected to a parallel path containing the required amount of loss to equalize the levels. In the case of subband level modulation (H3), a separate device of this type must be used in each subband.

The system just described operates on a total energy basis. Sometimes it is possible to obtain a switching signal on the basis of energy frequency distribution. Consider, for instance, the system using two different displacements (B2). The alternate positions of the speech band are illustrated in Figure 10. In one position, the band is right side up and occupies the range from 2 to 5 kc. The alternate position is inverted occupying the range from 3 to 6 kc. Since most of the energy in the speech band is concentrated in the low-frequency part of the original spectrum most of the time, the system illustrated in Figure 11 can be used to decode this material automatically. The signal is applied to two band filters, one covering the range 2 to 3 kc, the other passing 5 to 6 kc. The out-

puts of these band filters are rectified individually and fed to the two windings of a polar relay. The relative energy in the two band filters will be different for the two displacements and the relay in Figure 11 will be operated alternately in the two directions, thereby automatically connecting the proper carrier to the input modulator in Figure 7 to put the speech band in its normal position. This will not be infallible, but with displacements as different as the ones used in the illustration, it should operate sufficiently well to yield most of the intelligence of the message. Naturally, the smaller the physical difference between the two positions being distinguished, the more false operations there will be. However, this method is instantaneous even with an irregularly switched system, whereas cryptographic methods would be very time-consuming.

Another variation of this general technique might be mentioned for the sake of completeness although it is somewhat more speculative. Consider a privacy system which depends on speed changes (F4). Changes in speed cause changes in the pitch of the voice. Suppose we apply this signal to a circuit which measures the voice pitch. This technique has been worked out in connection with the Vocoder. The output of this circuit, which is a varying frequency, is used to change the speed of a motor. The motor is part of the drive of a magnetic tape recording and reproducing system through which the signal is passed. As the motor speed is made to change, the tape speed changes in such a direction as to tend to keep the derived frequency constant. This takes out not only the speed variations, but also the voice inflections. However, a monotone is quite intelligible.

The following method, which has not yet been tried out, is intended to apply to irregular band displacements or wobbles (B4), which would be exceedingly difficult to handle any other way. Consider a system in which the band is kept right side up, but is wobbled over a range sufficient so that demodulation with some intermediate carrier frequency will not give an intelligible signal. Suppose the wobble follows an irregular, nonrepeating program. The following decoding method is proposed.

The signal is impressed on a network having a very steeply rising loss characteristic. If the speech band were not wobbled, this network would simply tend to make the lowest harmonic of all voiced sounds the strongest component. With the wobble, the same thing will be true except that the level of this component will

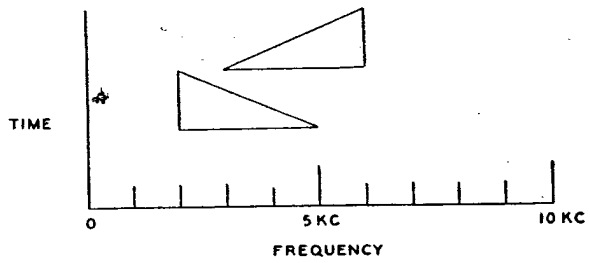



FIGURE 10. Sidebands in two-position displacement system.

undergo severe fluctuations. Therefore, the resulting signal is subjected to some form of automatic volume control and also a limiting action, tending to derive a single frequency. Forgetting voice inflections for the moment, this derived frequency would fluctuate up and down (in frequency) in step with the band wobble. In fact, it could be used as a subcarrier in a double modulation decoder to demodulate the signal to approximately the correct position in the frequency range. It will be in error,

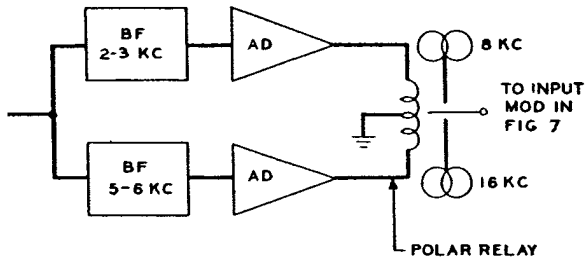



FIGURE 11. Automatic decoding system depending upon energy-frequency distribution.

however, by an amount equal to the instantaneous voice pitch. Possibly this amount of error will not prevent the signal from being intelligible (we know that this amount of displacement does not destroy the intelligence of otherwise normal speech).

If it is desired to correct for this error, two methods suggest themselves. One possible method is to subtract from the derived frequency, by a modulation process, an amount

equal to the average pitch of the voice being monitored. This will leave a small fluctuating error. Another possibility is to derive the actual instantaneous voice pitch, by difference tone methods, and subtract this amount from the derived subcarrier frequency.

If the displaced band is inverted instead of right side up, a similar procedure can be used, with a network of opposite loss characteristics. In either case this method will correctly demodulate only the voiced sounds, but experience suggests that this is sufficient. If not, some kind of carry-over effect might be incorporated in the system to prevent sudden changes in the subcarrier frequency, thereby tending to hold over correct demodulation for short unvoiced sounds also. This method has not been tried, but is felt to be worth recording because of the great difficulty of handling irregularly wobbled systems by any other method.

Another rather speculative automatic method might be mentioned because some form of it might prove useful against certain multiplication systems such as H1. The code wave in the particular case encountered was repeated many times per second, and there was a synchronizing pulse ahead of each cycle. If the signal is applied to a synchronized cathode-ray oscilloscope with a highly persistent screen, a definite pattern appears because the coding wave always passes through zero at the same time. Also, the speech energy tends to average out after a few cycles so that the pattern reflects the amplitude of the coding wave. It is quite conceivable that this pattern on the screen could be scanned optically and used to generate a decoding wave for automatically unscrambling the signal. Obviously, if the coding wave is changed periodically, a new decoding wave is automatically produced. The only requirement is that the coding wave persist long enough to form an average pattern on the screen.

Another variation of automatic decoding methods might be termed "parallel-automatic" because two or more complete decoding units are used in parallel but only the correct one is applied to the listening receiver. To emphasize the difference between this method and the one previously discussed, we will use the same example, namely, the system with two band displacements. Referring to Figure 7, suppose instead of the parallel modulators, there were two complete units in parallel including the band filter, the second modulator, and the output filter. One of the units is fed with the 8-kc carrier, the other with the 16-kc carrier. Each unit will have straight speech in its output half the time, and the other half the time will have inverted speech displaced by 1 kc. A 1-kc low-pass filter can then be used in a device similar to Figure 11 to switch the listener to whichever one of the decoding units has the straight speech. For the particular system used in the illustration, there does not appear to be any particular advantage of one method over the other. However, the latter system can be applied in cases where the other method might not be feasible.

The parallel-automatic method can be made to give a different type of switching signal. For instance, use might be made of the harmonic relationship between the components of speech when the speech band is in its normal position. If the voice pitch happens to be 100 cycles, then all the harmonics will be multiples of 100 cycles. If this speech is put through a suitable nonlinear system such as a rectifier or limiter, difference tones will be generated which will also be multiples of 100 cycles. If, however, the speech band is displaced from its normal position in any way, the difference tones will not coincide with the speech components. If, for instance, the whole band has been displaced by 50 cycles, then the speech components will be 150, 250, 350 cycles, etc. The difference tones generated by a nonlinear system will be 100, 200, 300 cycles, etc. If we now take a second difference between the output of the nonlinear system and the original components, there will be generated multiples of 50 cycles. The lowest component of this series will be lower than the pitch of the voice. This will be true regardless of how far the original band has been shifted, except for the special case where the shift happens to be an exact multiple of the voice pitch. Since, however, the pitch is constantly varying, this coincidence is of very brief duration. Theoretically, at least, a low-pass filter with a cutoff lower than the normal range of voice pitch can be used as a clue to determine whether a speech band is in its proper location. The method then would consist in having sev-

eral decoders in parallel, listening only to the one which did not generate a component in the low-pass filter.

The above illustrations will serve to show the possibilities of noncryptographic types of attack on privacy systems. When a new system is encountered, this type of attack should be given serious consideration because of the saving in time and equipment. Naturally, as pointed out above, straightforward cryptographic attack can be made to yield a better quality signal. However, experience has shown that the ear can become familiar with certain kinds of distortion and learn to extract the intelligence more and more readily with practice.

TABLE 1. Summary of scrambling systems.

| | Noncryptographic attacks (Table 2) | Capable of cryptographic attacks |
|---|---|---|
| A. Single modulation | | |
| 1. Inversion | 1a | .... |
| 2. Variable frequency inversion | 1b, 2a, 2f | .... |
| 3. Alternate inversion | 1b, 2f | .... |
| 4. Phase reversal | 1b, 2e, 2g, 3e | * |
| 5. Split phase | 1a | .... |
| B. Double modulation | | |
| 1. Fixed displacement | 1a | .... |
| 2. Stepped displacement | 1b, 2a, 2f, 3b, 3f | .... |
| 3. Wobbled displacement, regular | 1b, 2a | .... |
| 4. Wobbled displacement, irregular | 3d | * |
| C. Triple modulation | | |
| 1. Re-entrant inversion, steps | 1b, 2c, 2f | .... |
| 2. Re-entrant inversion, continuous | 1b, 2a | * |
| D. Band splitting | | |
| 1. Slowly switched | 1b, 2b, 2f, 2g, 2h | * |
| 2. Rapidly switched | 2c, 2f, 2h | * |
| E. Time division multiplex | | |
| 1. 4-band system | 1b, 2b | .... |
| 2. With noise channel | 1b, 2b | .... |
| F. Magnetic tape | | |
| 1. Delayed subbands | 2b | .... |
| 2. TDS, repeated code | 2c, 2g, 2h | * |
| 3. TDS, nonrepeated code | ..... | * |
| 4. Speed variations | 1b, 2a, 3c | * |
| 5. Backwards transmission | 1b | .... |
| 6. Alternate backwards and forwards | 1b, 2c | .... |
| G. Tape plus modulation | | |
| 1. TDS and inversion | 2f, 2g, 2h | * |
| 2. TDS and split band, synchronous | ..... | * |
| 3. TDS and split band, nonsynchronous | ..... | * |
| 4. Two-dimensional | ..... | * |
| 5. Double-speed split | 1b | .... |
| 6. Half-speed split | 1b, 2c | .... |
| H. Wave form distortion | | |
| 1. Multiplication | 2b, 2e, 2g, 3e | * |
| 2. Level modulation | 2d, 3a | * |
| 3. Subband level modulation | 2d, 3a | * |
| J. Masking methods | | |
| 1. Signal plus noise, same direction | ..... | * |
| 2. Signal plus noise, opposite direction | 2i | .... |
| 3. Tone sequence | 1b, 2b, 3a, 3b | .... |
| 4. Noise spurts | 2c, 2d, 3a | .... |
| 5. Nonlinear distortion | 1a | .... |
| K. Vocoder methods | | |
| 1. Permute channels | ..... | * |
| 2. Invert channels | 1b, 2g | * |
| 3. TDS channels | 1b, 2g | * |
| 4. Two-dimensional scramble | 1b, 2g | * |
| 5. Time division multiplex | 1b | * |
| L. Channel mixing | | |
| 1. Time division mixing | 2c, 2f | * |
| 2. Subband mixing | 2b | * |
| 3. Combination | 2c, 2f | * |

TABLE 2. Noncryptographic decoding methods.

1. Captured set or functional equivalent
   a. Fixed condition—find by trial
   b. Simple program—get into step
2. Compromise decoding methods
   a. Intermediate condition
   b. Listen to portion of frequency band
   c. Listen part time
   d. Limiter, peak chopper, compressor
   e. Rectifier
   f. Superposition
   g. Approximate code by trial
2. (*Continued*)
   h. "Spoil" good code by recoding
   i. Directional discriminator
3. Automatic decoding
   a. Total energy
   b. Energy frequency distribution
   c. Pitch-change corrector
   d. Wobble corrector
   e. Code wave generator
   f. Parallel automatic
   g. Inharmonic detector

In general, noncryptographic methods require that the signal, as received, be of fairly good quality. In some cases, the saving in time, labor, and equipment would be so great that if the signal, as received, is too poor to permit noncryptographic attack, the most reasonable thing to do is to move the intercept station to get a better signal.

In Table 1, there is listed for each privacy system, the type of noncryptographic attack which might apply. It should be emphasized once more, however, that the method which succeeds at one switching speed may fail at another. The list, therefore, should be taken only as a recommendation of systems which should be considered. The noncryptographic decoding methods are summarized in Table 2.

## 4.4 CRYPTOGRAPHIC TOOLS AND METHODS

A cryptographic decoding method involves (1) actually determining a code which will undo the scramble, and (2) restoring the speech by means of this code. In the case of repeated codes, this can sometimes be done rather quickly. An example is the repeated-code TDS system. The actual codes used can be found in about 15 min. Having found the code, we can set it into our receiving machine and thereafter listen to the speech directly. In the case of nonrepeated codes, every bit of the message must be handled individually. It may take a thousand or even a hundred thousand times as long to decode as it did to speak the words. It may take hours or even days to obtain the intelligence from a short message; meanwhile other messages will have been sent and we get farther and farther behind. The only way this could be avoided would be to have approximately as many teams working in parallel as the ratio of decoding time to message time, which, of course, is impractical if the ratio is large.

As stated previously, the sound spectrograph —described in detail later—is of tremendous assistance in recognizing the nature of an unknown scrambling system. The ear can usually recognize the presence of time discontinuities. It can also recognize the peculiar quality which results from band-shifting systems. The exact nature of the scramble, however, is usually impossible to establish with the ear. Even scrutiny of the wave form may yield no clue. The strikingly graphic analysis provided by the spectrograph, however, usually takes the mystery out of the scrambling method immediately.

For example, speech privacy systems having frequency subbands will show horizontal discontinuities or boundaries in their spectrograms. Similarly, systems employing time division will show vertical boundaries. A considerable variety of systems display both horizontal and vertical boundaries. Methods of telling these systems apart are described in the final report on Project C-32.[44]

### Program Determination

The simplest cases to handle are those involving a program which can be determined directly from spectrograms by inspection or measurements. The re-entrant inversion system (C1) might be used as an example. Suppose a multiplicity of displacements were used in some irregular sequence. Discontinuities marking the inversion frequencies appear in the spectrograms and once they have been determined by measurements on a large number of spectrograms, the program can thereafter be determined quite readily by using a template. This template can be marked directly with the settings of the decoding machine which will restore the speech to its normal position.

Another example involving a program would be one like B2, in which two different displacements are used alternately, with the intervals irregular in duration. Here the time boundaries will be quite apparent and they can be measured with a suitable time scale.

In all likelihood changes of the above types will occur in discrete steps for practical reasons. The use of a program involving continuous changes with time presents formidable technical difficulties at the authorized as well as the unauthorized terminals.

### Matching Spectrograms

In cases where the scrambling system involves rearrangement of the speech elements in time or in both time and frequency, the basic

method for determining the codes involves cutting up spectrograms along the element boundaries and rearranging the elements so as to restore the straight speech. An example is shown in Figure 12. The criterion for rearranging the elements is that there should be continuity at the boundaries. This continuity includes the position and direction of the individual harmonics, the position and direction of the resonance areas, and, in general, the amplitude as represented by the darkness or lightness of the patterns. The pieces are numbered before the matching process begins and when the matching has been completed, the numbers on the pieces determining the code.

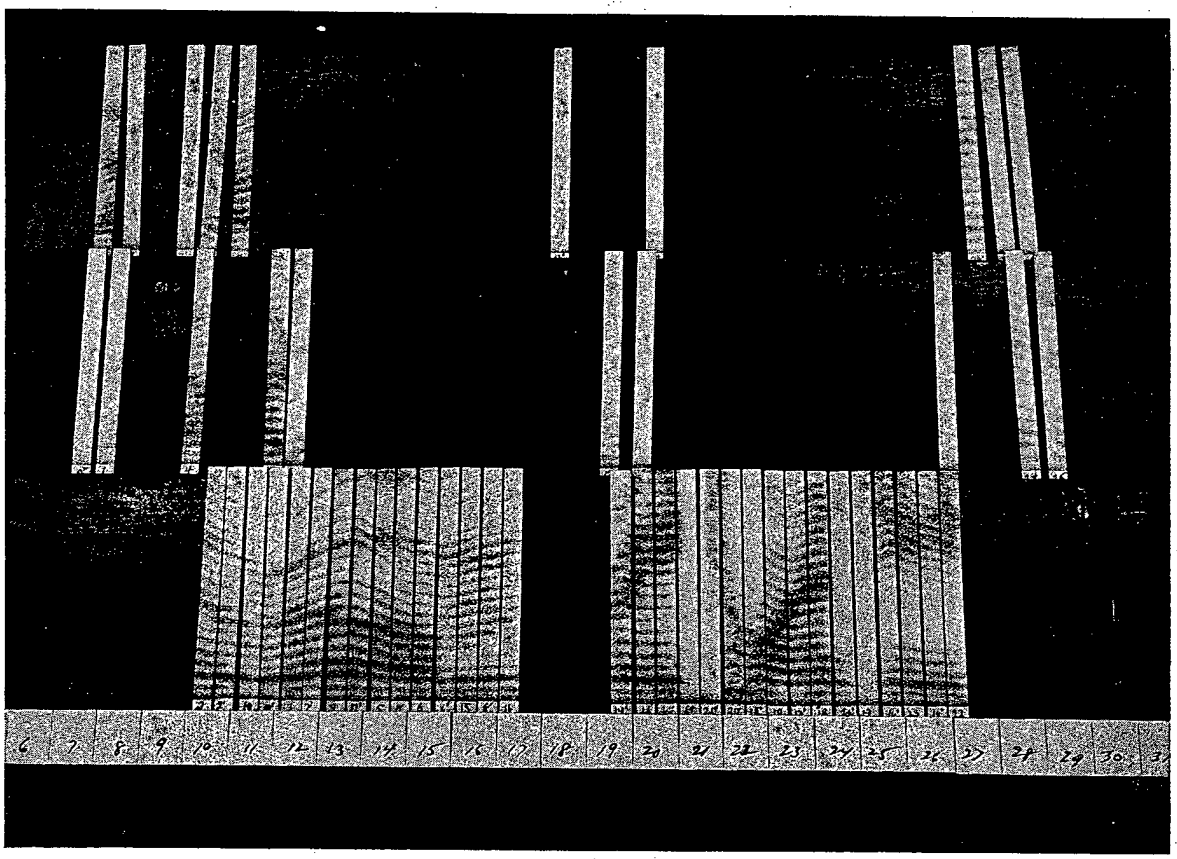


FIGURE 12. Method of matching spectrograph patterns of nonrepeated code TDS.

If the scrambling process involves inversion of the time or frequency scales, straight speech can be restored for matching purposes by making two spectrograms as shown in Figure 13. Present models of the spectrograph include means for making a mechanically inverted pattern as well as a normal pattern. The spectrogram at the top of Figure 13 shows a normal pattern. Directly below it is an inverted pattern of the same material. A mechanically inverted pattern is indistinguishable from a pattern produced by electrical inversion of the speech. Similarly, if the whole inverted spectrogram is turned through 180 degrees, so that the base line is at the bottom and towards the observer, the result is indistinguishable from the case in which the speech is transmitted backwards. Therefore, if an element in the scramble is inverted, it may be recovered as straight speech for matching purposes by cutting the element from the mechanically inverted pattern. If an element has been transmitted backwards, it can be restored to normal by cutting it from the inverted pattern and rotating it 180 degrees as described above. If it is both back-

wards and inverted, it may be restored by cutting it from the regular pattern and turning it around.

It has been found from experience that matching is facilitated by enlarging the spectrograms by a factor of about two to one. Not only is the increased size easier to handle, but the heavy photographic paper is much better to handle than the facsimile paper employed in the spectrograph. The latter is delicate in texture and its surface is easily stained. In this connection it should be noted that the process of enlarging the spectrograms does not appreciably affect the decoding time in the case of nonrepeated code systems. There will, of course, be an initial delay, but in general, the matching time will be controlling. Spectrograms can be made, enlarged, and cut up faster than they can be matched. If it is found necessary, however, to use spectrograms for matching purposes regularly, then it may pay to adopt the technique described in Preliminary Report No. 13[17] (Project C-43) for producing large spectrograms photographically.

To facilitate matching, appropriate means should be used for handling the elements. It has been found that a slightly adhesive surface is advantageous. In the illustration of Figure 12 this surface was provided by coating the boards and also the backs of the elements with ordinary rubber cement. This is also the case in Figure 14. This latter example shows a two-dimensional scramble. Horizontal strips of rubberized Bristol board were provided for matching along the time axis.

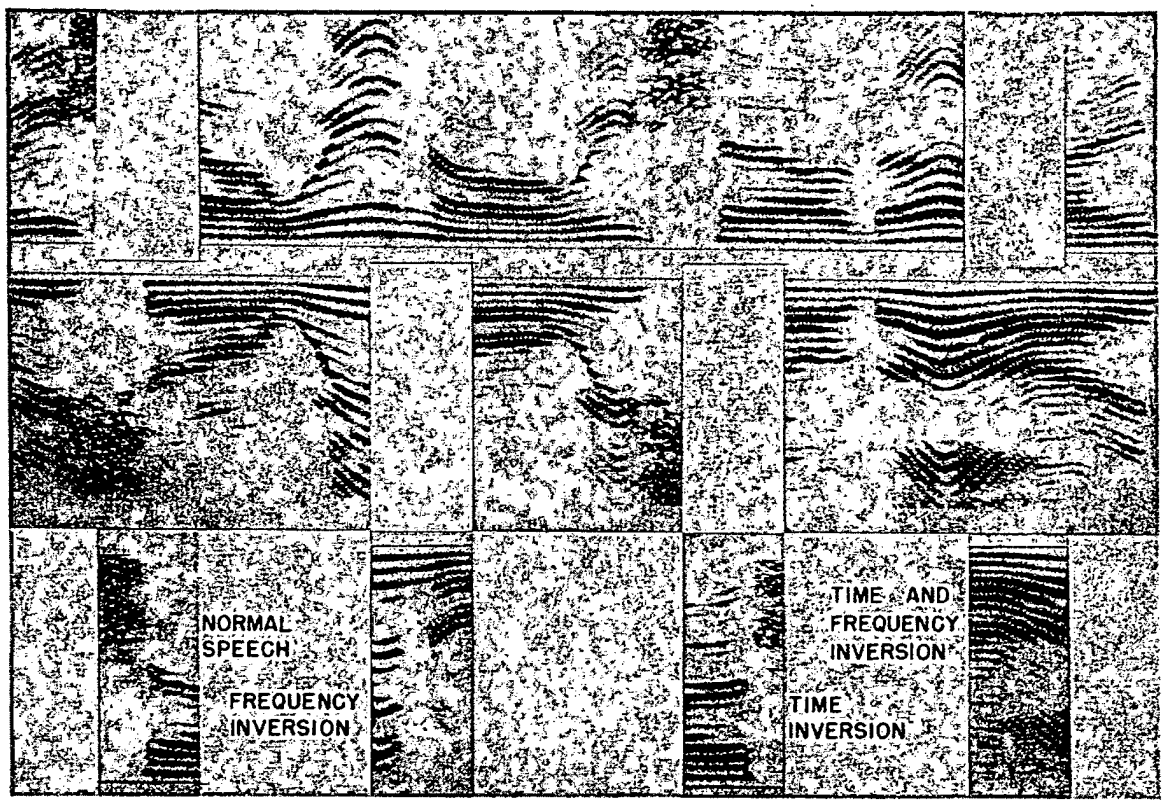



FIGURE 13. Inversion of time and frequency scales in spectrograms. If scramble contains inverted elements, these will appear right side up in mechanically inverted spectrogram. Time scale may be inverted by rotating elements 180 degrees. Note position of base lines in examples.

Once a system has been thoroughly diagnosed certain numerical properties of the coding process will be known. Advantage should be taken of this knowledge to supplement and check the matching process. Examples are given in Pre-

liminary Reports No. 10,[18] 14,[19] 22,[20] and 26[21] of Project C-43.

### Effect of Transients

The two examples thus far cited of spectrogram matching were artificially produced by cutting up spectrograms of straight speech, and the boundaries are therefore clear and sharp. In practice the time and frequency boundaries will be obscured by transients. Frequency boundaries are filter cutoffs, and they are marred by overlap or underlap and by phase distortion.

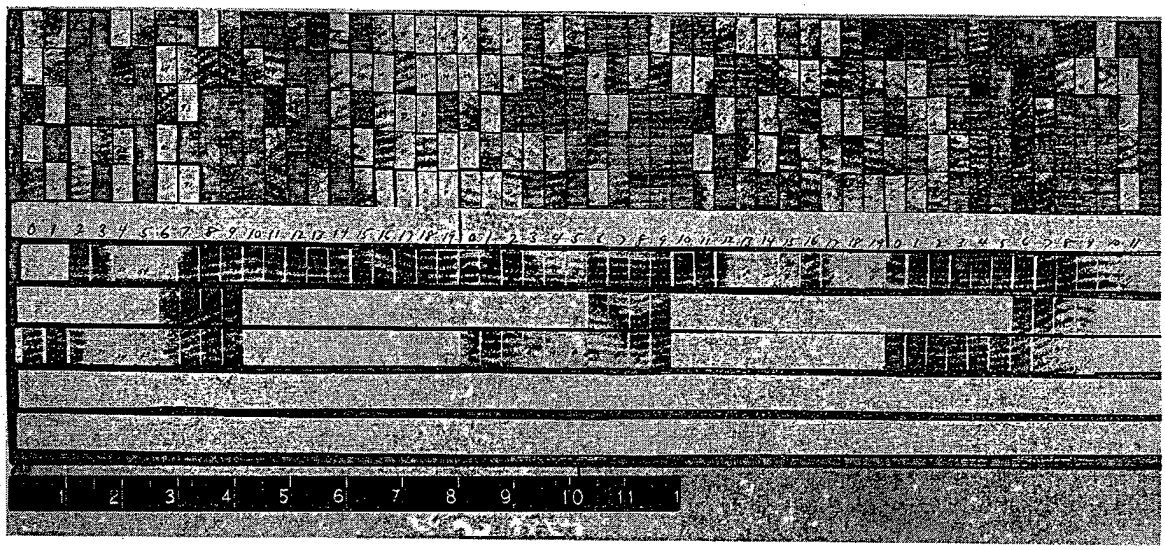



Figure 14. Matching spectrograph patterns of two-dimensional scramble.

This, however, is not as serious as the transients occurring at the time boundaries. There is a basic difficulty here, arising from the desire to obtain a high degree of frequency resolution, which entails the use of a narrow scanning filter. The response and decay time of such a filter is appreciable in comparison with the element length in many scrambling systems. The decay time produces the more serious of the two effects. It causes energy from a strong element to spill over into the adjacent following element in the spectrogram. This difficulty is unlikely to cause trouble in any application of the spectrograph except decoding. Therefore, it is felt that means for alleviating this difficulty should be recorded here. A small amount of exploratory work has been done along these lines, but the embodiment of this improvement in a spectrograph has not been accomplished because the need was not sufficiently pressing in Project C-43.

The basic idea for avoiding the obscuring effects of spillover is to permit the spillover to take place in such a way as to be subsequently removable. For instance, suppose a sample of TDS were recorded on the magnetic tape and suppose the spectrograph were equipped with a suitable switching arrangement such that only every alternate element was reproduced. The spillover from each element would then occur in a blank area, and it could subsequently be trimmed off, leaving a sharp, clear boundary. A second spectrogram could then be made of the alternate elements, again trimming off the spillover.

### Use of Two Scanning Filters

A logical extension of this idea, which would save some time, would be to have two scanning filters and use them alternately by suitable switching means. Both the inputs and the outputs of the filters would have to be switched, and the two switches should be separated by the appropriate time delay to take account of the transmission time through the filter.

A third variation of this idea which requires

less equipment, is to make one spectrogram in the usual manner and then make a second spectrogram with the machine running backwards. The spillover always occurs into the leading edges of the elements in spectrograms. Cutting the first spectrogram in the proper places will result in clear, sharp right-hand edges on each element, but each left-hand edge will be obscured by spillover. Cutting the second spectrogram in the proper places will give clear left-hand edges on each element. Matches could then be made between elements from the normal and backwards spectrograms, in such a way as to utilize the good edges of the elements.

In other respects it is to be expected that the patterns produced by the spectrograph can be improved. For instance, studies have been made which show that amplitudes can be represented in such a way that they can be interpreted quantitatively. This is an improvement over the rather indefinite shades of gray in the usual spectrograms. It would provide another criterion for matching. In some cases, however, this might be a handicap. For instance, in TDS systems the pole pieces are not all of equal efficiency. The amplitudes of adjacent speech elements are affected by this change in efficiency and they might not appear to match when they really should. This condition, of course, might be aggravated intentionally as part of the privacy feature of the system. On the whole, however, it looks as though amplitude representation should be an improvement in decoding work.

### Matching Variable-Area Patterns

For some purposes it has been found that wave form patterns offer certain advantages over spectrograms. They can be made more rapidly and they can be played back directly to reproduce the original speech. Intrinsically, wave form patterns are not as good as spectrograms for diagnosing frequency shifts and the like. However, they present the time scales more graphically and they are not subject to transients at time discontinuities such as the spillover effects previously discussed.

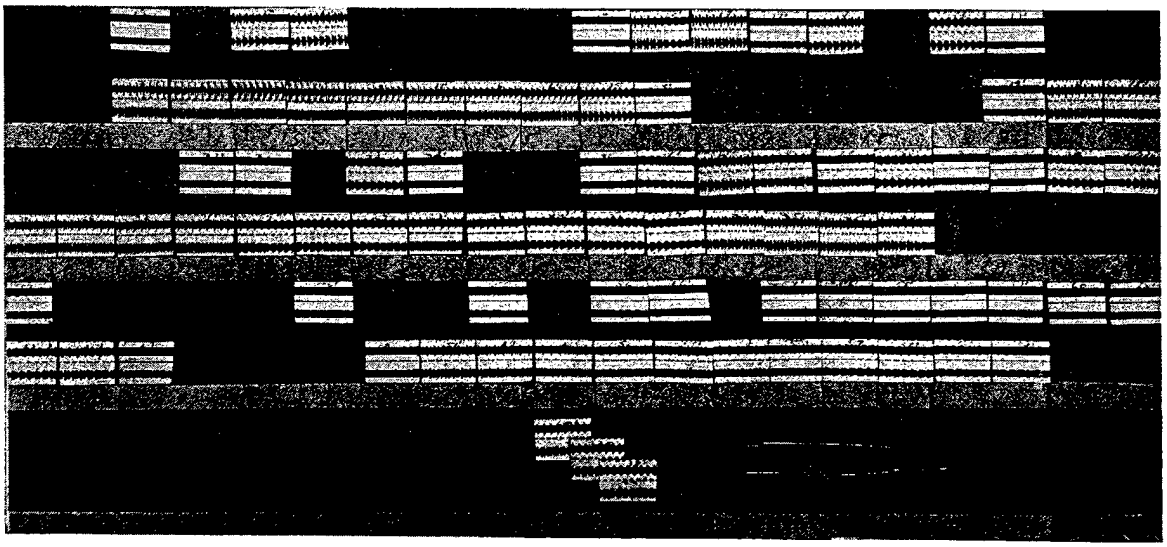


FIGURE 15. Matching variable-area patterns of nonrepeated code TDS.

The particular type of wave form pattern found most useful was a variable-area pattern similar to the sound track used in moving pictures. Variable-area patterns are more distinctive to the eye than oscillographic traces. They form geometric designs that catch the eye and facilitate matching. The manner of producing and playing back these patterns is described in Preliminary Reports No. 1,[22] 7,[23] and 12[24] of Project C-43. An example of variable-area patterns in process of matching is shown in Figure

15 taken from Preliminary Report No. 26[21] of Project C-43.

Variable-area patterns of this type have been found particularly good for decoding TDS systems, especially repeated-code systems. Amplitudes are clearly represented in these patterns. By matching a multiplicity of cycles of a repeating-code system simultaneously, it is possible to take advantage of this amplitude representation even though the wave form itself might be obscured by other features of the privacy system. For instance, the use of split-band coding was once proposed to increase the privacy of TDS systems. This combination would be much more private than plain TDS if judged on the basis of matching spectrograms, particularly if the split-band codes were rapidly switched at intervals not simply related to the TDS elements. No difficulty, however, was found in matching the variable-area patterns to find the TDS code. This is described in Preliminary Report No. 19[25] which also describes a scheme for nullifying the effect of split-band coding on the wave form. This consists of modulating all the frequency bands down into one frequency band. Changes in the split-band code will then have no effect on the wave form of patterns produced in this manner.

It was also proposed at one time that the use of a whisper or monotone instead of normally inflected speech would increase the privacy of TDS systems. Again this is true in terms of spectrograms, but it was found that variable-area patterns could be matched almost as easily for whispered speech as for normal speech, and with the monotone it was actually easier. This is described in Preliminary Report No. 16[26] of Project C-43.

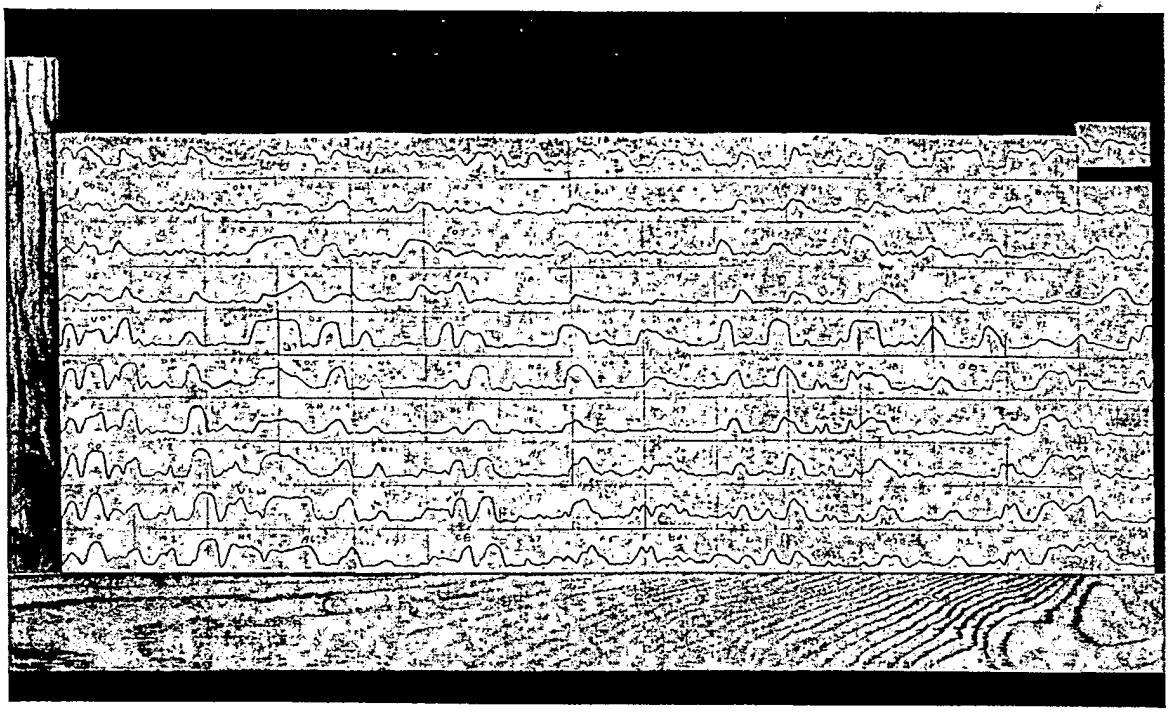


FIGURE 16. Oscillographic traces of Vocoder channel signals.

Another feature of the variable-area patterns which might be useful is that the patterns have characteristic shapes. Usually they look like a series of damped oscillations with the highest amplitude at the beginning of each fundamental period. This should enable the recognition of cases in which speech is transmitted backwards. The characteristic periodicity of the patterns might also be used to recognize whether a frequency band is in its proper location.

Toward the end of Project C-43 it came to be recognized that there would be considerable ad-

vantage in using a compressor in the production of variable-area patterns. This tends to bring out low-level sounds. The distortion of the wave forms resulting from instantaneous compression is immaterial if they are to be used only for matching. This kind of compression, however, should be sharply distinguished from automatic volume control action. The latter is relatively slow acting and it is obvious that in TDS systems, for instance, it would alter the amplitudes of certain elements in such a way as to make matches impossible.

### Matching Oscillograms

Oscillographic traces can be used instead of variable-area patterns, although in general there will be a disadvantage. For Vocoder privacy systems, however, oscillographic traces are required. The signals in Vocoder channels are essentially fluctuating d-c signals after they are modulated down to their normal frequency location. They can best be examined in the form of oscillographic traces. Figure 16 shows a set of undistorted Vocoder channel signals. It will be noted that there is a tendency for the amplitudes to vary simultaneously in the several tracks. It has been found that if the signals in the various channels are permuted, even with the sharp edges resulting from artificially produced scrambles, the number of mismatches tends to be about 40 per cent. This means that a Vocoder system with its channels permuted at short intervals provides a rather difficult privacy system to decode.

It has been found that compression enhances the value of oscillographic traces of this type. Without compression the lower amplitudes are obscured by the width of the traces. Instantaneous compression makes changes in the magnitude or direction of the traces apparent in the lower level sounds. The patterns shown in Figure 16 were produced in this manner.

### Indicator Methods

In the following methods a visual indication is obtained denoting which of several possible choices puts the speech elements in their proper order. These methods are applicable only to cases where the possible number of choices is not overwhelmingly great. A natural example of a visual indication occurs in the illustration of TDS in Figure 17. Whenever two originally adjacent speech elements remain adjacent in the scramble the two elements are not separated by a time boundary in the spectrogram. Elements which do not belong in adjacent positions have a boundary resulting from discontinuities in the harmonics and from spillover effects. The absence of a time boundary can be taken as an indication that the two adjacent elements belong together. To make use of this effect the following procedure is suggested. Record a sample of the scramble on a loop of tape. Reproduce this sample through a TDS machine

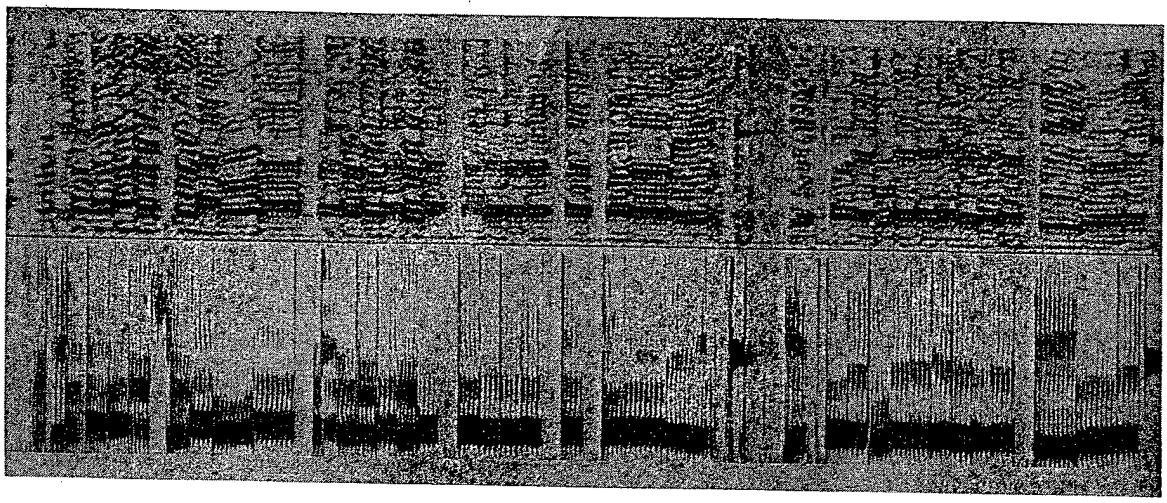


FIGURE 17. Time division scrambling [TDS].

and make a spectrogram, noting any adjacencies which occur. Change the code in the TDS machine and make another spectrogram again noting adjacencies. A systematic set of codes should be worked out in advance which explore all the possible combinations of elements. At the end of such a cycle of operations it should occur at the boundaries of elements which do not belong together. These will generate frequencies higher than the cutoff of the high-pass filter and will appear as pulses on the scope. The absence of a transient will indicate either that the elements belong together or that no energy was present. Again a systematic cycle

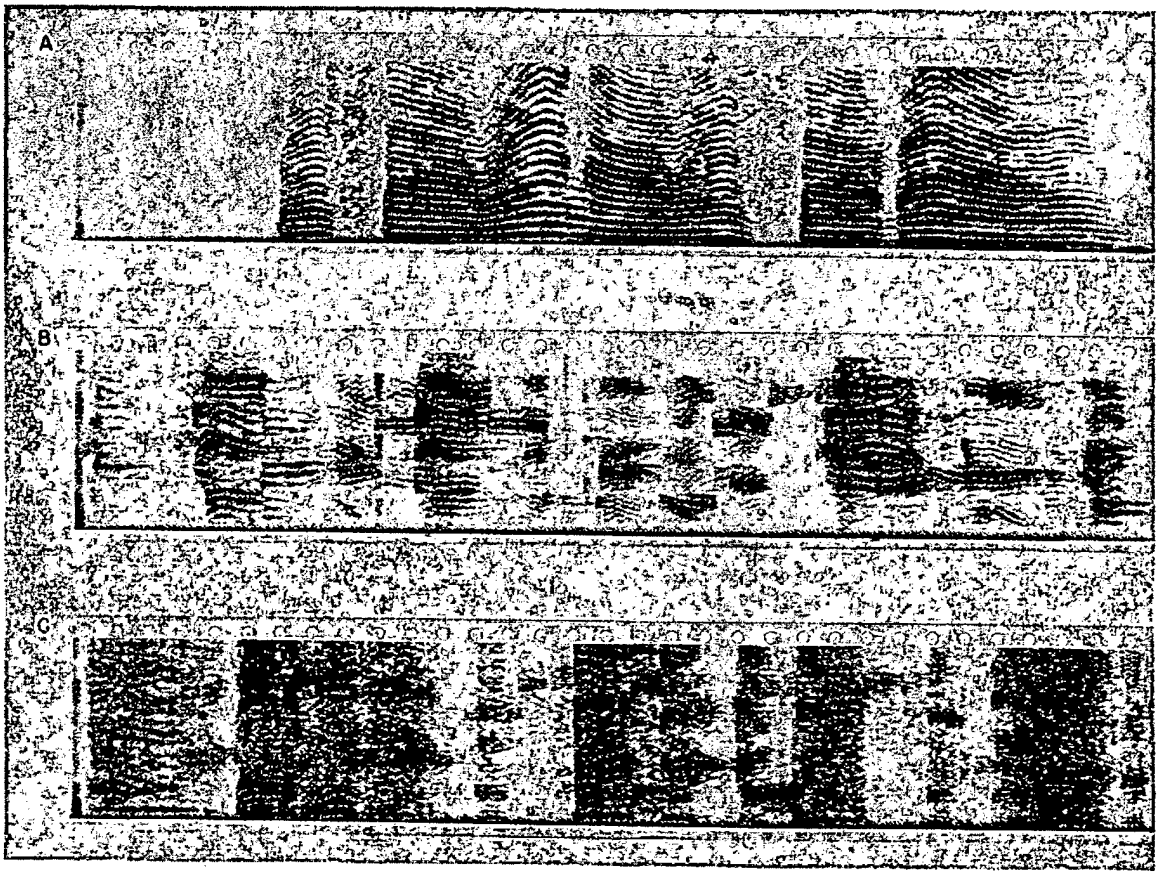



FIGURE 18. Effect of rectification on normal and band-shifted speech. A, straight speech rectified; B, six-code split-band scramble; C, effect of rectifying six-code split-band scramble.

be possible to place a large percentage of the elements correctly. This can be applied to non-repeated or repeated code TDS.

A variation of this method, which was suggested but not tried and which should be much faster, is as follows: Reproduce the recorded sample through a low-pass filter, say 2,500 cycles. Pass it through a TDS machine and then through a high-pass filter with the same cutoff. View the output of the high-pass filter on a cathode-ray oscilloscope whose sweep is synchronized with the TDS cycle. Transients will of codes should place most of the elements correctly.

Another example of the indicator method is the following: Suppose in a split-band D2 system six known codes are used in an irregular sequence, and it is desired to determine the sequence. The following procedure is suggested: Record a sample and reproduce it through a decoding machine equipped with one of the proper decodes, and make a spectrogram. Certain elements in the spectrogram will be seen to be normal speech. These elements,

of course, are the ones to which the particular code applies. It is much easier to determine whether a particular element consists of straight or scrambled speech, than to determine which particular code was used. Repeat this procedure with each of the other five codes. Each element can thereby be identified with a particular code.

USE OF RECTIFICATION

A variation of this procedure, which should give more positive results, is as follows: The

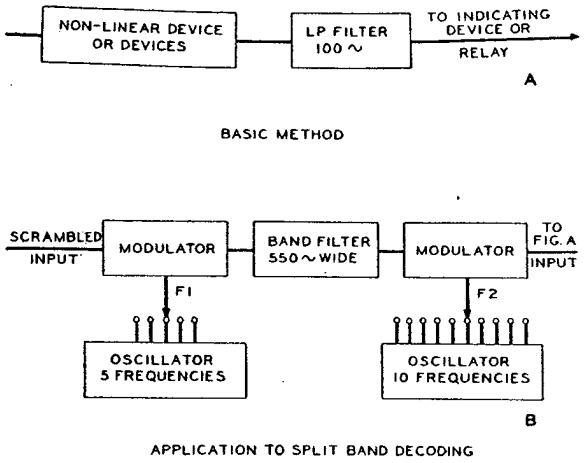



FIGURE 19. Band-shift detector.

output of the decoding machine used as above is rectified before making the spectrogram. Rectifying normal speech does not add inharmonic components, whereas rectifying speech which contains band shifts results in inharmonic components. This is illustrated in Figure 18. The upper spectrogram shows rectified straight speech. This looks perfectly normal except that the frequency range is somewhat more completely covered with harmonics than is the case in normal speech. The second spectogram shows a sequence of split-band scrambles. The third spectrogram shows a similar sample rectified, with none of the elements decoded. Rectifying the undecoded elements results in a complete smear in the spectrogram compared to the rectified straight speech. Properly decoded elements will stand out more clearly against the background of rectified scrambled speech.

Another variation of the indicator method consists in subjecting the scrambled speech to a nonlinear device or devices in such a way as to obtain difference tones between the components. In normal speech, in which all components are harmonically related, there will be no difference tone lower than the pitch of the voice. In scrambled speech the components are not harmonically related and there will be difference tones lower than the pitch of the voice. The output of a 100-cycle low-pass filter therefore, can be used to indicate whether a band of speech is in its proper frequency location or not. This is illustrated in Figure 19A. The importance of this method lies in the fact that each frequency band can be examined separately. It might therefore be used to determine for each element in a two-dimensional scramble which frequency band it came from.

Figure 19B shows how each band can be lifted out of the scramble and placed in each of the five possible positions either straight or inverted. The spectrograph might be used to speed up the analysis process as illustrated in Figure 20. The output of the low-pass filter is fed to the marking amplifier. Whenever the output of the low-pass filter is zero there will be no mark produced. Whenever there is an output a mark will be produced. The procedure would then be as follows: Set oscillator F1 at one value and then set oscillator F2 successively at each of its ten values (or five if inversion is not required). Repeat with oscillator F1 at each of its other five values. For each of these 50 settings allow the spectrograph drum to rotate two or three times with a few blank rotations between each setting. The traces on the drum will then look something like the drawing. The time axis is as usual disposed lengthwise. If all the traces in a given time interval are blank it is presumed that this represents a silent interval. Single blank intervals in otherwise continuous marks indicate that these settings were the correct ones. If none of the marks for a particular element are blank the indications are that at that particular moment a consonant occurred which of course is composed of inharmonic components. This system was not actually tried in this complete form but enough work was

done to show that it is possible to make use of the presence of inharmonic components in some such manner. It appears therefore that a substantial fraction of the elements in a two-dimensional scramble might be identified as to frequency location.

One other possibility of this type might be mentioned. Variable-area patterns of vowel sounds have characteristic configurations. These configurations depend on their harmonic structure, and a disturbance of this structure

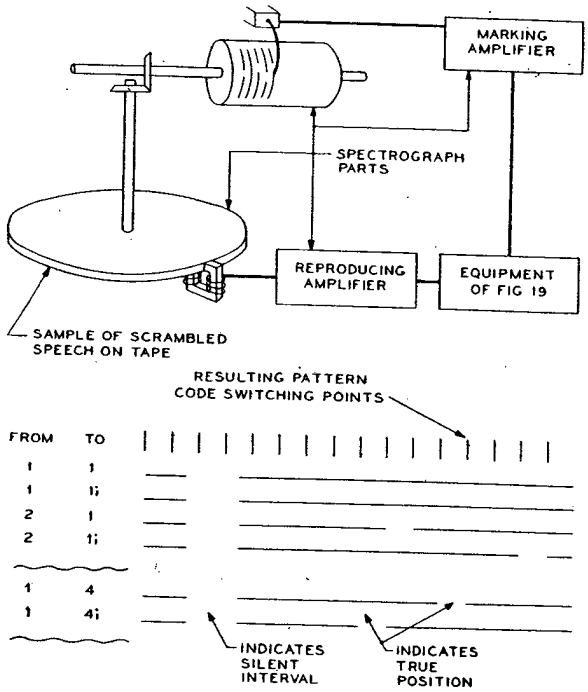



FIGURE 20. Adaptation of spectrograph for decoding switched split-band scramble.

should change these patterns in a recognizable manner. For instance, if the components are inharmonic there will be no periodicity at the fundamental pitch rate. It might therefore be possible to use variable-area patterns, which can be produced much more rapidly than spectrograms, as indicators along the lines of the above discussion.

## APPLICATION TO TABLE 1

In this section we will examine the application of cryptographic methods to the specific scrambling systems listed in Table 1. In this table the systems which might require cryptographic attack are indicated. The following paragraph numbers refer to privacy systems in Table 1.

A4. Among the systems listed under single modulation the only one that might require cryptographic treatment is the phase-reversal system. This system is a special case of the multiplication system which will be treated later.

B4, C2. Among the double and triple modulation systems, the irregular continuous displacements were not handled by noncryptographic methods. It might be necessary to make a continuous series of spectrograms to determine the displacements as a function of time. This might someday be done continuously and instantaneously, in which case compensating frequency changes might be made continuously by hand to decode the material.

D1, D2. Among the band-splitting systems, the fixed or slowly switched codes can be solved by inspection. If the code is rapidly switched, however, single elements seldom contain sufficient information to determine the codes. If the switching sequence is a repeated sequence, it may be worthwhile for the sake of quality to determine the sequence and get in step with it. In this case the methods described under the heading "Indicator Methods" should be of assistance. If the switching sequence is never

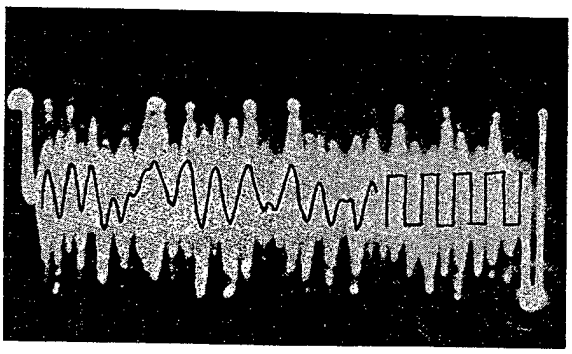


FIGURE 21. Repeated code multiplication system.

repeated the indicated noncryptographic methods appear most reasonable.

F2, F3. TDS systems yield very poorly to noncryptographic attack. For repeated-code systems, however, the code can readily be determined by matching either spectrograms or

variable-area patterns, taking advantage of the numerical properties of the codes. These methods are covered in Preliminary Report No. 14[19] of Project C-43. Nonrepeated-code systems, however, have thus far been found exceedingly difficult to handle, although the methods of spectrogram matching, matching variable-area patterns, and indicator methods apply. Efforts in this direction are described in Preliminary Report No. 26[21] of Project C-43.

F4. Speed variations, according to some preliminary laboratory tests, are rather ineffective in masking the intelligence of speech unless the variations are exceedingly wide and rapid. Technical difficulties then become so great that this appears to be an unlikely privacy system by itself. Small variations in speed, however, might be used to make spectrograms of TDS systems more difficult to match. In this case, however, it will be unnecessary to determine the speed variation program if the TDS scramble can be removed.

G1, G2, G3. Combinations of TDS and frequency scrambles are interesting from the cryptographic standpoint. Since repeated-code TDS systems were found easy to break, it was proposed to add various forms of split-band scrambles. It was argued that the continuously changing frequency scrambles would alter the shapes of variable-area patterns so that they could not be matched. Furthermore the changing frequency scrambles would make spectrograms unsuitable for matching, especially if the split-band codes were switched nonsynchronously compared with the TDS boundaries. Each time the frequency code was switched a new vertical boundary would appear in the spectrogram, and in combination with the TDS boundaries the spectrograms would be very severely broken up in the time scale. It was found, however, as discussed in Preliminary Report No. 19[25] of Project C-43, that if the TDS code is a repeated code the frequency scrambles can be practically ignored in matching variable-area patterns. Having found and removed the TDS code the remaining frequency scramble can be solved by noncryptographic methods.

In the case of nonrepeated TDS, however, the addition of split-band coding would increase the difficulty considerably, provided that the two coding systems do not provide clues to each other. The most promising method for handling this system appears to be to determine the split-band codes first by the indicator methods previously discussed. If the split-band codes are then removed the remaining scramble can be handled as straight TDS. Another possible method is to make variable-area patterns with all the decodes superposed. The resulting patterns, however, will not be as satisfactory for matching as patterns of straight speech.

G4. The two-dimensional scramble can be handled by matching spectrograms if a repeated code is used. Experiments along these lines are described in Preliminary Report No. 22[20] of Project C-43. If the code is nonrepeated, however, it would be exceedingly difficult and time consuming to handle by unaided matching. It would help considerably if the original frequency location of each element in the scramble could be determined. This might be accomplished by the methods described under the heading "Indicator Methods."

H1. Determining the code for multiplication or phase-reversal systems can be accomplished quite readily if the code is repeated at sufficiently short intervals. In the one system which was met in Project C-43 (Preliminary Report No. 18[27]) the code wave was repeated 100 times per second. In this case the scrambled signal could be applied to the vertical plates of an oscilloscope with the horizontal sweep synchronized with the code cycle. It is obvious that every time the coding wave passes through zero the scrambled signal also passes through zero regardless of the value of speech signal at the moment. If several cycles of scrambled speech material are superposed, therefore, they have the appearance shown in the photograph, Figure 21. The superposed traces show a definite pattern, with regions of high and low amplitude, and also sharp indentations. These latter are the crossover points of the code wave. There is also a marked tendency for the peaks to occur alternately above and below the center line, but the amplitudes of the peaks are not all alike. Since the speech amplitudes tend to average out over a number of cycles, the amplitudes of the superposed peaks reflect pretty accu-

rately the amplitudes of the coding wave at those points. The probable shape of the coding wave based on this evidence, has been partly traced in.

It has been found experimentally that if only the crossovers of the coding wave are reproduced the speech will be intelligibly decoded. The decoding wave need not be the reciprocal of the coding wave. It can be like the one drawn in at the right in the photograph. It is only necessary, therefore, to generate a wave having its crossovers at the indicated points, and reverse the phase of the scrambled signal of these points.

H2, H3. Level modulations by themselves are not private, but they might very well be used in combination with other systems in an attempt to foil the matching of speech patterns. The level modulations themselves, however, need not be solved cryptographically.

J1. There appears to be no method either cryptographic or noncryptographic for breaking the noise-masking method if the noise is predistorted, random, and sufficiently high in level to really mask the speech. These requirements, however, make the technical difficulties for system operation very great and it is unlikely that this method can be used over radio channels. Cracking this system therefore becomes a matter of solving the noise-distorting system. Project C-43 had no experience along these lines.

K1, K2, K3, K4. Scrambled Vocoder channels can theoretically be solved by matching oscillograms. Actually as mentioned under the heading "Matching Oscillograms" this procedure is very difficult because the channels look so much alike.

L1, L2, L3. Channel-mixing systems would be exceedingly difficult to handle cryptographically if a sufficient number of channels were involved so that noncryptographic methods were inapplicable. The only possible method of attack appears to be matching spectrograms. Since, however, about 25 per cent of normal speech consists of pauses, many of the switch points will occur in these pauses and it will therefore be difficult to establish continuity by matching.

### Determination of the Message

The objective of decoding work is usually not to determine the codes used, but to learn the intelligence which was transmitted under these codes. In the case of repeated-code systems, the procedure for obtaining intelligence is obvious once the code has been determined by the methods outlined above. It is only necessary to set this code into a machine similar to that used at the receiving end of the system being monitored, and listen directly to the transmitted speech. If the material has been recorded while the code was being determined, the recorded material can in general be decoded in the same way.

In the case of nonrepeated-code systems, the determination of the code sequence leaves us in general a long way from the determination of the message. All the material must first be recorded in scrambled form. It is necessary during this process to establish time reference points in the scramble, perhaps by superposing clicks or spurts of tone during the recording process, and referring the code sequences to these points. A decoding machine must be available, such as the one described in Preliminary Report No. 15[28] of Project C-43, which is adaptable to a variety of coding systems. The code sequence must be set into this machine, perhaps in the form of a punched tape. The scrambled material must then be reproduced and fed into the machine, maintaining proper synchronism between the reproducing and decoding systems. This is a formidable job.

There are some alternative possibilities which may apply in special cases. In the case of nonrepeated-code TDS, for instance, the process of matching variable-area patterns has actually restored the speech in reproducible form. Variable-area patterns can be played back just like the sound tracks used with motion pictures.

### Use of Playback

A playback machine of this type is described in Preliminary Report No. 12[24] of Project C-43. The rearranged elements are mounted on a strip of adhesive, and scanned with a light slit and photocell. Considerable noise is caused by

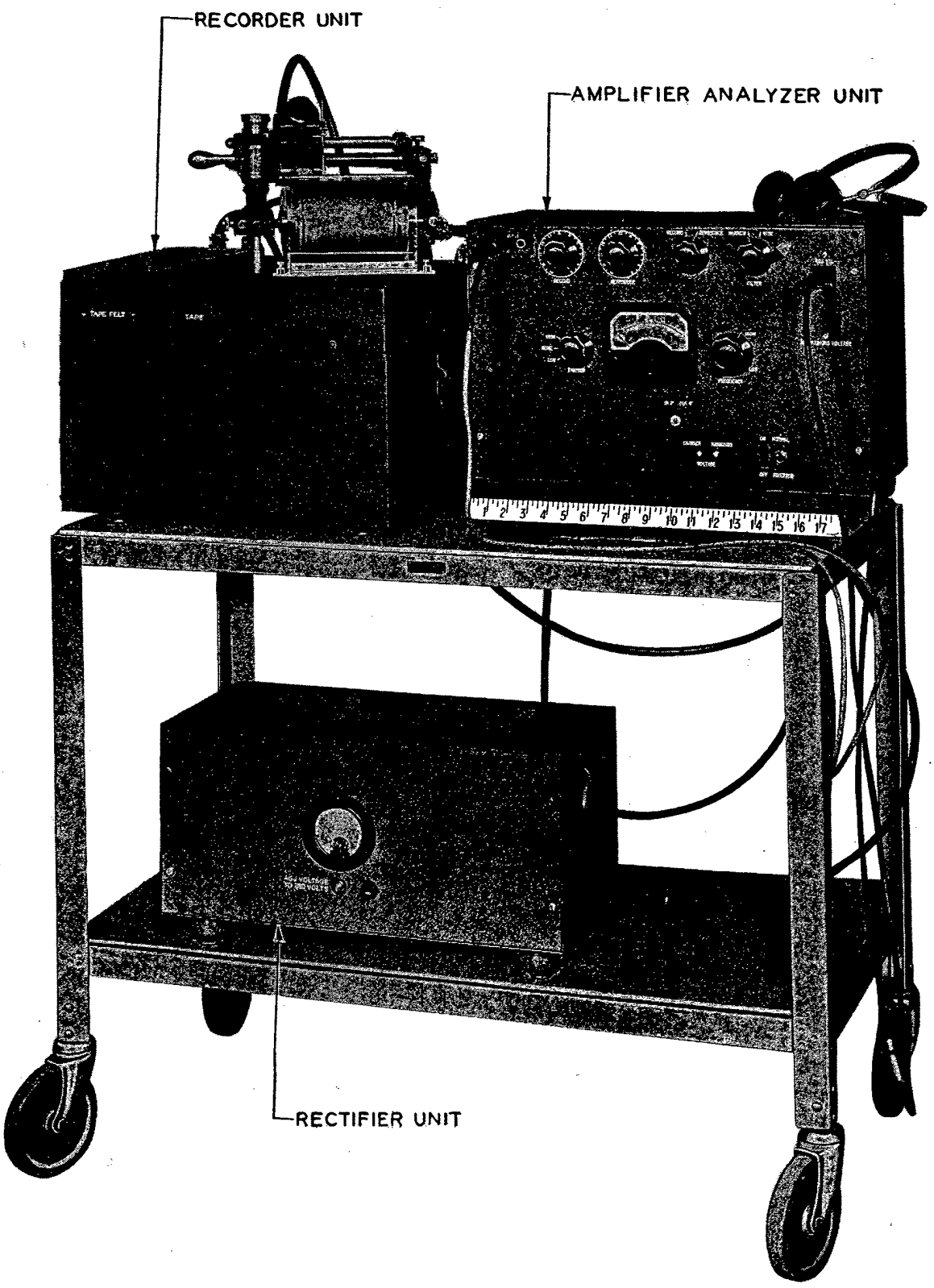



FIGURE 22. Sound spectrograph (D-165529) on a "push-around."

SECRET

the joints between the separate elements, but this could be largely eliminated by a specially designed squelch circuit, perhaps controlled by a separate light beam and photocell to cut off the output wherever a joint is passing under the scanning beam. The first attempt to use this decoding method was unsuccessful, as discussed in Preliminary Report No. 26[21] of Project C-43. However, there is nothing basically wrong with the method; it simply needs better execution than it received in the first attempt.

If the solution of the coding system requires spectrograms rather than variable-area patterns, it is still theoretically possible to play back the rearranged pieces. A playback machine for spectrograms is described in Preliminary Report No. 17[29] of Project C-43. This first model requires a negative transparency of the spectrograms, to be scanned by a light slit and photocell, with a multifrequency light chopper interposed ahead of the photocell. Again the method is basically sound. The experimental machine described in the report needs considerable improvement before it will yield adequate quality for the purpose described above, in order to overcome the degradation of quality caused by the joints, by slight misplacements of the elements, by spillover at the boundaries, etc. Furthermore, to get good patterns for matching, the signal must be subjected to a very high degree of compression, which distorts both the time and the frequency distribution of energy. It may be necessary to make one kind of pattern for matching, and another kind for playback, as was done with the variable-area patterns described in Preliminary Report No. 26[21] of Project C-43.

As a final alternative, it is possible to learn to read speech spectrograms by visual inspection. Theoretically, therefore, the rearranged spectrograms might yield the message directly. Here again, however, the boundary distortion will increase the difficulty of reading the patterns. It has also been found that the best patterns for matching are not the best for reading, and it may be necessary to make two sets of patterns. However, since spectrograms have been continually improving, the possibility of visually determining the intelligence from rearranged spectrograms must be listed as a distinct possibility, and one which, if it is feasible, is the most general of all methods since the basic procedure is the same for all the scrambling methods which can be handled in this manner.

## 4.5 THE SOUND SPECTROGRAPH

In the material to follow describing the sound spectrograph developed in Project C-32 and used continuously in subsequent decoding and evaluating projects, a brief and general description will be followed by a more detailed analysis of this important visual aid to the study of privacy systems. The sound spectrograph analyzes speech (or other sounds) in terms of its three basic dimensions of time, frequency, and amplitude. Such analyses, shown visually on a graph or chart, are helpful in understanding the complexities of sound and what various scrambling methods do to speech to make it unintelligible.

In March 1941 an early laboratory model of the sound spectrograph was demonstrated as an instrument that with further development might be useful in studies of telephone privacy. It was appreciated at that time that the need might arise for intercepting communications in scrambled speech and decoding them. It was also appreciated that new scrambling systems might be encountered and that means would be needed for diagnosing such systems. For such a purpose the unaided ear has very limited capabilities. Such things as oscillograms, which show the wave form, provide few clues as to the mechanism by which the wave form was changed. Project C-32, the forerunner of Project C-43, was organized in the fall of 1941 to produce a sound spectrograph useful for diagnosing and decoding speech scrambling systems.

About a month before the attack on Pearl Harbor, patterns that could be used for decoding work were being produced with a breadboard model, and the first finished model of the spectrograph was available by the end of that year. Additional models of the spectrograph were built for the Armed Services, incorporating improvements in operation and in rugged-

ness. The model, described in the final report of the Project C-43 and shown in Figure 22, has been used in studies of various privacy systems submitted by the Army, Navy, and NDRC for the purpose of evaluating the degree of security which they afforded. Improvements in the form of a calibrating circuit built into the spectrograph and control circuits added in the form of an appliqué unit, were made as the work progressed.

### 4.5.1 How the Sound Spectrograph Works

A schematic diagram of the sound spectrograph is shown in Figure 23. The signal to be analyzed is recorded on a loop of magnetic tape at a speed of 25 rpm permitting a sample 2.4

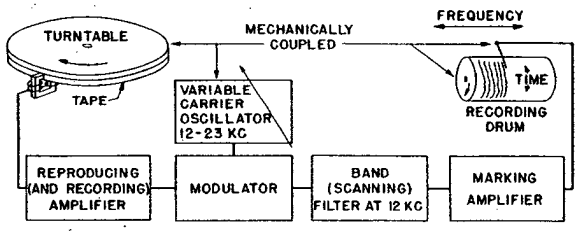



FIGURE 23. Schematic diagram of sound spectrograph.

sec long to be recorded. The recorded material is then reproduced at 78 rpm. Because of this speedup, the original signals which may have filled the frequency region between zero and 3.5 kc now extend to about 11 kc. The signal is modulated with a carrier which gradually changes in frequency from 23 to 12 kc as the recorded material is reproduced repeatedly. The lower sideband of the resulting signal is passed through a band-pass filter with a center frequency of about 12 kc.

The output of the filter is amplified and fed to a stylus bearing on facsimile paper, making a trace varying in density with the instantaneous energy passed by the filter. The paper is mounted on a drum which is geared to the turntable rotating the magnetic tape. As the frequency of the modulating carrier changes, the stylus moves along the drum laterally. The resulting spectrogram is built up line by line. In this manner a pattern is produced which shows by its light and dark areas how the intensity in the signal varies as a function of time and frequency.

The change in frequency produced by modulating the voice signal with a varying carrier signal of suitable high frequency would not be necessary if it were possible to make a band-pass filter whose center frequency could be shifted easily. In this case the actual voice frequencies could be scanned by the filter to determine the characteristics in frequency with time. It is easier, however, to accomplish the same object by the method actually used in the spectrograph.

### 4.5.2 Operation

It is the fact that both time and frequency variations are simultaneously displayed which makes spectrograms so valuable for decoding work.

Scanning filters of various widths can be used for different purposes. If the filter is wide, it will give an analysis which is limited in the amount of detail it can portray in the frequency dimensions, but it will respond quickly to changes in amplitude with time, and will therefore give sharp time resolution. The narrower the filter the more frequency detail is shown in the spectrograms, at the sacrifice, however, of some of the time resolution. With all the filters thus far used, the shift in frequency range from line to line is only a fraction of the width of the filter. Successive lines in the spectrogram, therefore, do not represent successive frequency bands. They represent frequency ranges which overlap by a large fraction of their total width. The density of the patterns, therefore, changes very gradually along the frequency dimension.

The kind of patterns produced by this method of analysis is illustrated in Figure 24. The upper spectrogram in the figure was made with a scanning filter about 300 cycles in width. The separate words can be plainly distinguished. The vowels are distinguished by dark bands with vertical striations. The consonants are in general less intense and show a different type of structure. It will be noted that the dark

bands are different in the different vowels, and they change not only from one word to the next but also within each word. Analyses of this type, therefore, graphically portray changes in the energy frequency distribution of a complex signal with both time and frequency. It should be emphasized, however, that the relative intensities of the various components of this particular sample of speech, notably the consonants, differ to a far greater extent than would be judged by the relative blackness of their patterns. In other words, a very large amount of level compression is incorporated in these patterns.

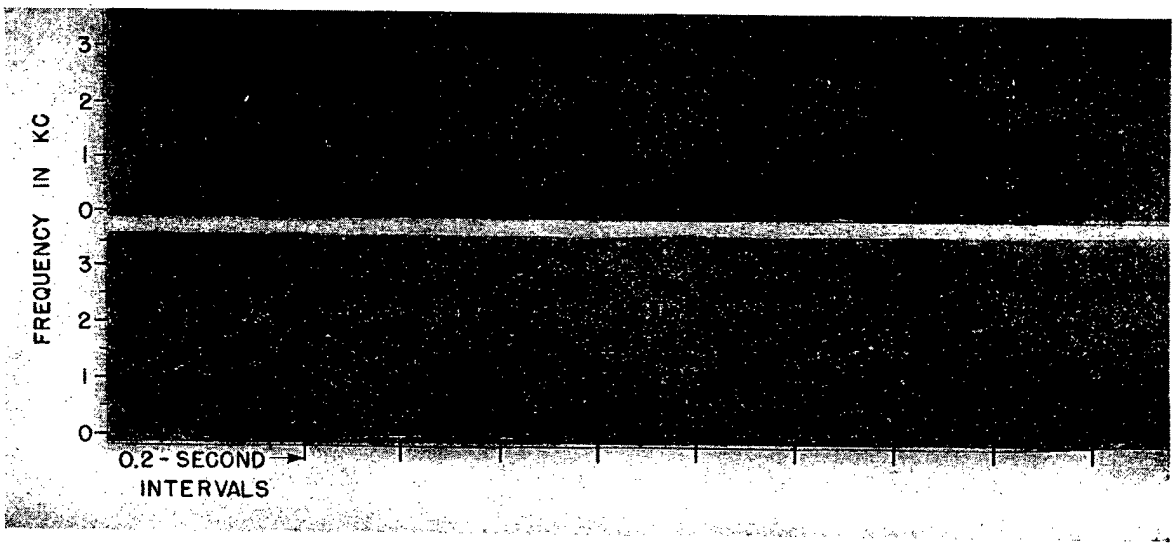



FIGURE 24. Spectrograms of normal speech, words being "one, two, three, four, five, six." In this case, spectrograms are somewhat smaller than normal size due to photographic reduction and some trimming at ends.

The lower spectrogram in the figure shows the same words analyzed with a filter only 45 cycles wide. This filter is narrow enough to resolve the individual harmonics of which vowel sounds are composed. The harmonics consist of the fundamental voice pitch together with both odd and even multiples of this frequency. Some of the harmonics are stronger than the others, because they are reinforced by resonance in the oral cavities as the words are formed. It will be noted that the dark areas in these patterns correspond in frequency and in trend with those in the upper spectrogram. The fact that vowel sounds consist of discrete harmonics causes the vertical striations in the patterns made with the wider filter. Whenever the filter is wide enough to pass several harmonics at once, these harmonics beat with each other and form maxima and minima in the output of the filter. The frequency of the beats corresponds exactly to the frequency of the voice pitch.

It will be noted in the 45-cycle spectrogram that the harmonics rise and fall in frequency from moment to moment. This reflects the changing pitch of the voice known as inflection. Inflection is normally used in connected speech, and this fact is of assistance in decoding work, because the spacing and trend of the individual harmonics in spectrograms provide important clues in diagnosing privacy systems.

### 4.5.3 Level Compression

In normal speech there is a tremendous change in level from moment to moment particularly in the level of consonants as compared to vowels. There is also a considerable difference in the average level at low frequencies as compared to high frequencies. This latter difference can be corrected by predistortion,

and present models of the spectrograph contain shaping networks for this purpose. There are, however, changes from moment to moment in the relative levels of high and low frequencies in different speech sounds which cannot be corrected by shaping networks. The facsimile paper on which spectrograms are made has a range of between 10 and 15 db. The range of levels in speech greatly exceeds this value. This means that if the average level is adjusted so that the highest components appear at maximum blackness, the lowest level components will be invisible. Conversely if the level is so adjusted that the low-level components appear in the pattern, the high-level components will severely overload the recording paper. To show both the high- and low-level components occurring in speech, therefore, it is necessary to compress the instantaneous signal into a much narrower range.

In the earliest models of the spectrograph the marking amplifier shown in Figure 23 was given a compressing action by means of a thyrite varistor across the grid of the output stage. Whenever the output of the scanning filter was low the gain of the amplifier was effectively raised from an average condition and whenever the output was high the gain was effectively lowered. This tended to equalize changes in level with both frequency and time. The compressor was replaced by devices which can exercise certain types of discrimination in controlling the instantaneous gain of the marking amplifier. These devices are known as control circuits. They provide patterns with better resolution in both time and frequency than can be obtained with the compressor. The patterns shown in Figure 24 were made with these control circuits in operation. The circuits are described in Preliminary Report No. 27[40] of Project C-43.

### 4.5.4 Possible Improvements

The spectrograph patterns underwent continual improvement in the course of this work, but probably they can be still further improved. The control circuits thus far produced are by no means the final word. Circuits of this type can be adapted to affect the patterns in various ways, and it is conceivable that different control circuits could be developed for decoding different types of scrambles.

One definite line of improvement concerns the time resolution. Many scrambling methods produce sharp discontinuities of the scrambled speech in the time dimension. The process of analyzing the scrambled signal in such a way as to obtain high frequency resolution tends to obscure the signal at these sharp boundaries. This is a basic situation which affects not only the spectrograph, but also all types of analyzers. To obtain a high degree of frequency resolution, a narrow filter must be used. The narrower the filter, however, the longer its response and decay time, that is, the output of the filter cannot be made to change as rapidly in level as the instantaneous level of the signal. This causes strong components to spill over across the time boundaries. In general this spillover does not interfere greatly with the recognition of various privacy systems, but it does interfere severely where spectrograms are to be used for decoding work. Several possible remedies for this situation have been devised and are recorded in Chapter VI of Part I of the final report of Project C-43.

### 4.5.5 Amplitude Representation

In the patterns thus far discussed the instantaneous intensity of the signal is represented by the lightness or darkness of the trace in the spectrograms. This representation is inherently nonlinear and practically impossible to make quantitative. For some types of work it would be highly desirable if the amplitudes could be represented in such a way that they could be interpreted quantitatively.

Figure 25 shows a spectrogram which upon close inspection will be seen to be made up of discrete dots. The dots are close together in the dark portions of the spectrogram and farther apart in the light portions. The dots themselves are all of equal blackness. The spacing of the dots is in fact quantitatively related to the instantaneous level of the signal. The level at any point in the spectrogram can,

therefore, be measured by measuring the dot spacing with suitable equipment and comparing it with a scale showing dot spacing vs level.

Another type of representation is shown in Figure 26. Here the levels are represented by the type of technique used in representing topographical variations in contour maps. The contour lines each represent regions in which the signal reaches a particular fixed level. The lines may be spaced so as to represent steps of any desired number of decibels, or any number of volts. In the lower spectrogram the spaces between the contour lines have been filled in with various densities of dot spacing. This permits instant recognition of equality of level in different portions of the signal.

Quantitative amplitude representation may or may not prove useful in decoding work. For certain kinds of signal it should prove useful, because it provides another dimension besides time and frequency which can be used for determining continuity or discontinuity in the signal. In other cases, however, it may prove useless, because changes in level have arbitrarily been introduced into the scramble.

The developments mentioned above emphasize the fact that the sound spectrograph is a highly flexible device and its capabilities along any line can be greatly increased by adding features designed for the specific purpose in mind.

### 4.5.6 Spectrograph Details

As described in general terms above, the output of the scanning filter of the sound spectrograph is recorded continuously on facsimile paper wrapped around a drum rotating with the magnetic tape so that one revolution of the tape corresponds to one rotation of the drum. The drum is moved laterally by a lead screw as the modulating frequency is slowly changed.

FIGURE 25. Method of representing amplitudes in such a way that they can be interpreted quantitatively by use of discrete dots all equally black. Dots are closely spaced in dark regions and widely spaced in light regions. There is definite quantitative relation between dot spacings at any point and level of signal at that point. Level could, therefore, be determined by measuring dot spacing.

The analyzer circuit comprises a variable-frequency oscillator, a balanced modulator in which the output of the oscillator is mixed with the voice frequencies, and the scanning filter. The balanced modulator automatically prevents any signals from getting into its output circuit except the resultant sidebands produced by the modulating or mixing process. Thus neither the original voice frequencies nor the oscillator frequencies appear in the output. Since the band-pass scanning filter has a mid-band frequency of about 12 kc it automatically selects or passes the lower sideband produced by the modulating process. The sidebands appearing

in the output of the modulator have energy-frequency distributions identical to the energy of the modulating signal and occupy a position in the frequency scale corresponding to the carrier frequency. A change in the carrier or modulated signal of, for example, —200 cycles, will cause the two modulator output sidebands to shift to a position in the frequency scale 200 cycles lower.

The scanning filter has a mid-band frequency such that when the carrier has one extreme value, only the lowest frequency components of the lower sideband will fall within the pass-band of the filter. When the carrier has its other extreme value, only the highest frequency components of the same sideband will pass through the filter. As the carrier frequency is slowly changed, all frequencies of one sideband (in this case the lower sideband) will be scanned by the filter and the relative strengths of the signals from moment to moment will be impressed upon the recording facsimile paper.

The record is made on what is known as Teledeltos paper whose light-colored surface is blackened by the passage of an electric current from the metal stylus through the paper to the metal drum on which it is wrapped.

In the model employed in Project C-43 and subsequent extensions of this project, the spectrograms are slightly over 12 in. long normally representing a recording of 2.4 sec making the time scale approximately 200 msec to the inch. The records are normally 2 in. wide covering 3.5 kc making the frequency scale about 1/16 in. per kilocycle. The frequency dimension can be expanded if desired but this requires that a longer time be available for making the record.

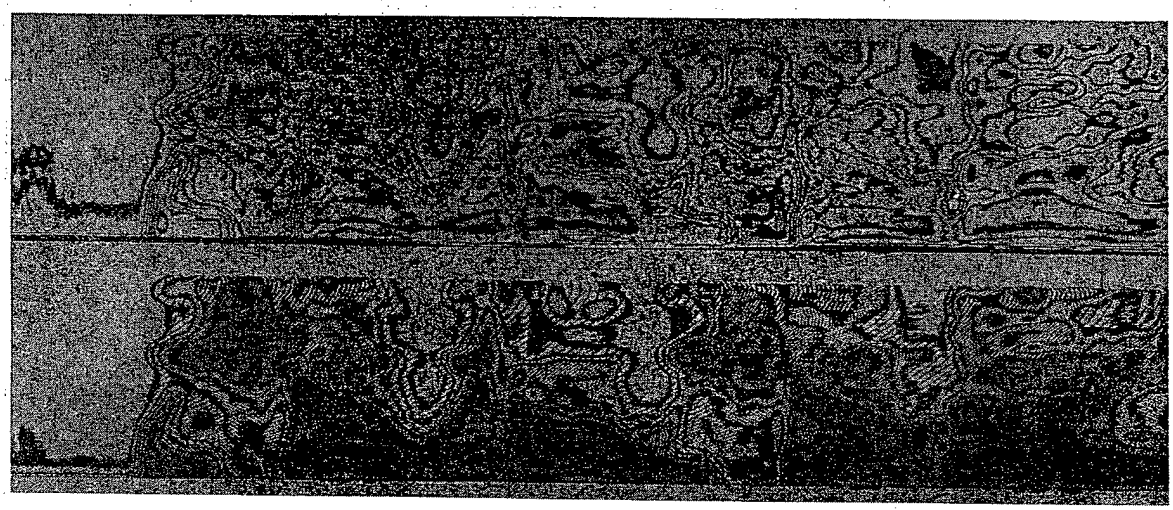


FIGURE 26. Amplitude representation by contours, every point on any one line representing equal signal level, and successive lines starting from blank background representing successively higher levels. In upper spectrogram, it is not immediately apparent which regions are peaks and which are valleys. In lower spectrogram, areas between successive lines have been filled in with patterns made up of discrete dots. Closer dots indicate higher level, with regions of equal level in different parts having same dot spacing.

### 4.5.7 Applications of the Spectrograph

Although the spectrograph was developed for use in analyzing speech privacy systems and in decoding scrambled speech records, it has more general application. The spectrograms shown here are characteristic of what the instrument can do in analysis and illustrate the results obtained with different filters, different scanning rates, and different types of material. The illustrations (taken from the October 1, 1943 report[41] on Project C-43) are for the most part familiar sounds selected to permit a mental comparison of the sound and its time-frequency pattern. These illustrations are followed by examples of the effects of various scrambles upon speech.

Perhaps the most familiar example of a wave

which is complex in both the frequency and time dimensions is speech, which therefore provides excellent material for illustrating what the spectrograph can do. Figure 27 shows a spectrogram of the sentence, "We shall win or we shall die," spoken in a normal manner by a male voice and scanned with the narrow filter. The time and frequency axes are indicated by appropriate scales. The intensity variations are indicated by variations in shade as shown in the scale below the spectrogram. It should be emphasized that there are about 400 horizontal scanning lines in this 4-in. spectrogram; too close together to be seen individually. The horizontal striations which do appear in the spectrogram are not scanning lines, they are the separate harmonics of the voice pitch, flowing up and down as the voice is inflected. The unstriated sounds are unvoiced, such as the "sh" in "shall."

Figure 28 shows spectrograms of the same sentence made with three different filters. In the one made with the widest filter, the separate harmonics are no longer visible, but the areas of resonance are brought out more clearly. Figure 29 shows a comparison between normal speech, a monotone, and a whisper, all by the same voice. In the monotone the harmonics are straight horizontal lines, and in the whisper the harmonics disappear almost entirely, but the dense regions by which the different sounds are recognized still persist.

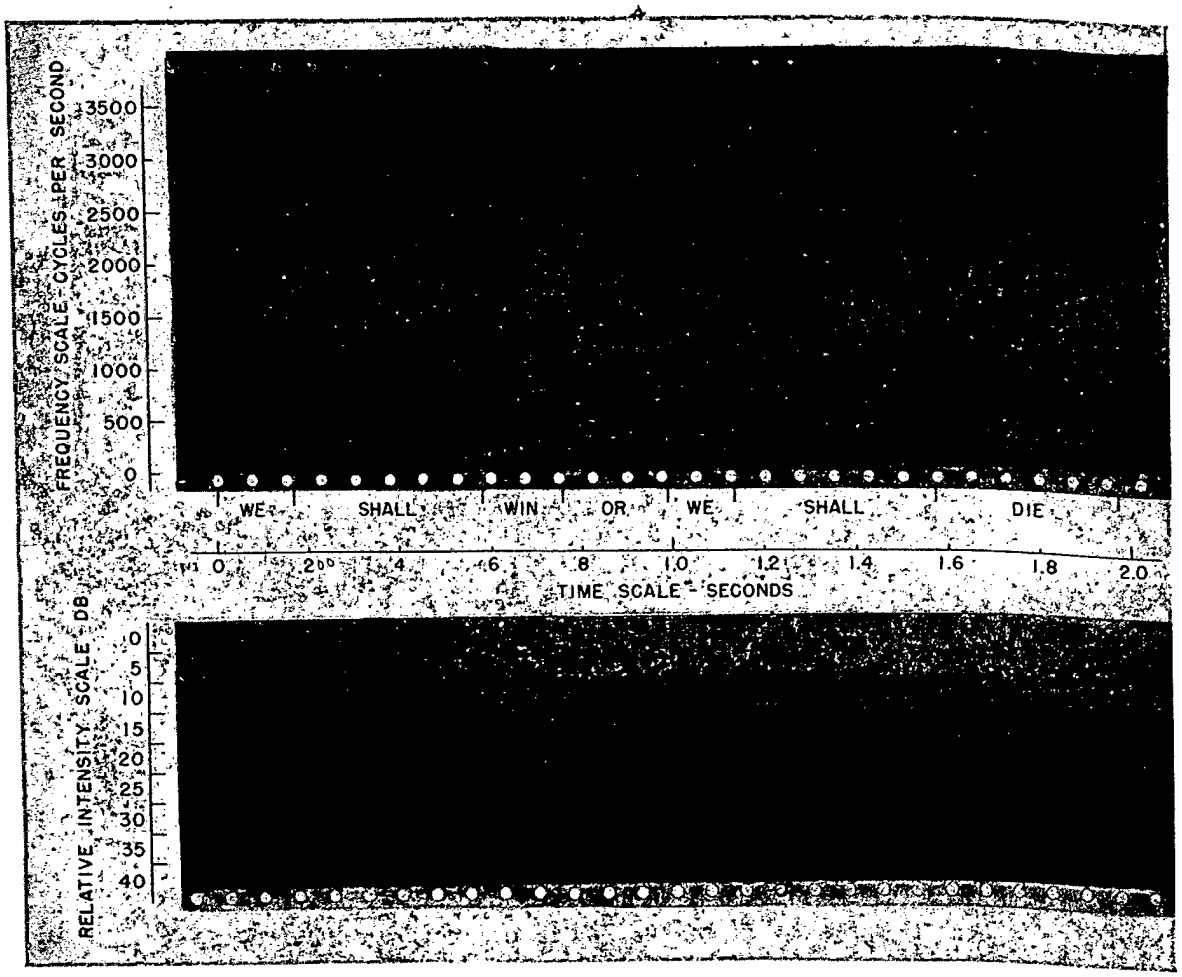



FIGURE 27. Spectrogram of "We shall win or we shall die," with "gray scale" below, showing intensity variation relation.

Figures 30 and 31 show some musical effects. The soprano solo shows how the vibrato affects both pitch and intensity. The harmonics, it will be noted, are much farther apart than in the male voice. In the piano music, the notes show tapering traces, as would be expected from their nature. The other illustrations require no special comment, except to note that the kc. The lowest spectrogram shows an acceleration measurement. It was desired to find how long it took a phonograph record to come to full speed after being released, the turntable running at full speed all the time. This was accomplished by simply recording an 8-kc tone on a sample record, and capturing the output of the reproducer during acceleration. The time

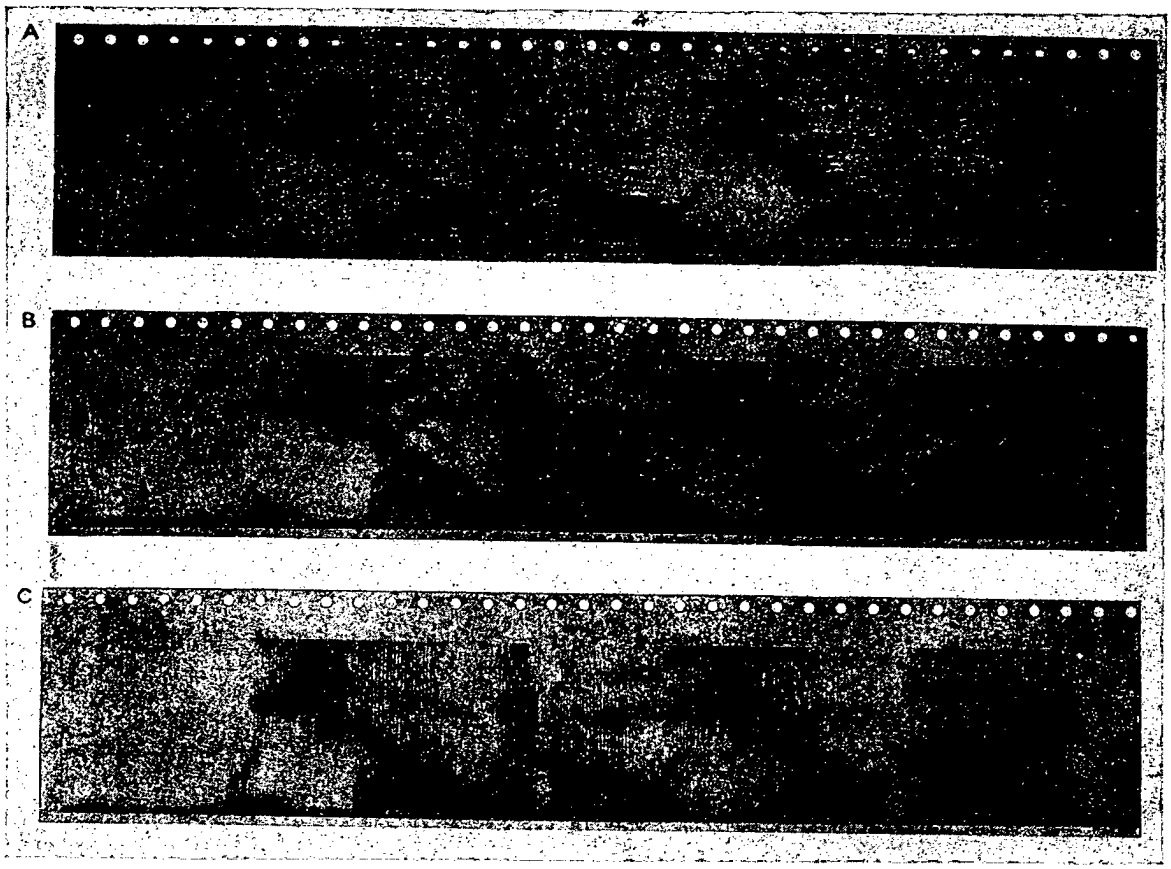



FIGURE 28. Same sentence as shown in Figure 27 recorded through filters of different bandwidths. A, with 45-cycle filter; B, with 90-cycle filter; C, with 300-cycle filter.

telephone bell was analyzed with the wide filter to show the time pattern more clearly. It may be seen that the clapper hits two bells alternately, but somewhat irregularly.

Figure 32 shows some applications in which the spectrograph provides a convenient method of obtaining a graph of frequency versus time. The upper spectrogram shows the output of a particular slowly warbling oscillator, and the second shows a more rapid sawtooth sweep frequency, the latter spectrogram covering 11 consumed in acceleration, 130 msec in this case, is directly indicated.

Figure 33 shows some more 11-kc spectrograms, illustrating the fact that some common sounds cover a very wide frequency range. Figures 34 and 35 return to the 3.5-kc range to show longer samples. They require no special comment.

Contrasting with these illustrations, Figure 36 shows an example of a steady wave, namely thermal noise. Two different levels are shown,

one of them analyzed with both the "narrow" and the "wide" filter. It will be noted that some of the sounds in the previously discussed spectrograms have components which are of the same nature as thermal noise, while some have components of definite frequencies. The latter can be recognized by their solid texture in the spectrograms as compared to the characteristic texture of a random wave form exhibited by thermal noise. The "sh" in "shall," and the roar of the flame, are examples of random sounds, while components of definite frequency may be seen in the jingling of keys (Figure 33) and the filing of metal.

These illustrations, which were chosen for variety and for interesting features, show what the spectrograph will do. Most of them, as emphasized before, show time variations as well as complex frequency structure because the ability to show both at once is the unique feature of the spectrograph.

### Speech Privacy Problems

Even in a steady flow of speech, the distribution of energy over the frequency range is constantly changing. Voiced sounds have a definite structure, consisting of a series of harmonics of the fundamental voice pitch, the harmonics being stronger in some frequency regions than in others. Unvoiced sounds have no such definite structure, but show a "smear" of energy which may or may not be concentrated in definite frequency regions. Words and sounds are recognized by their energy pattern in both time and frequency. Different speakers uttering the same sentence will produce pat-

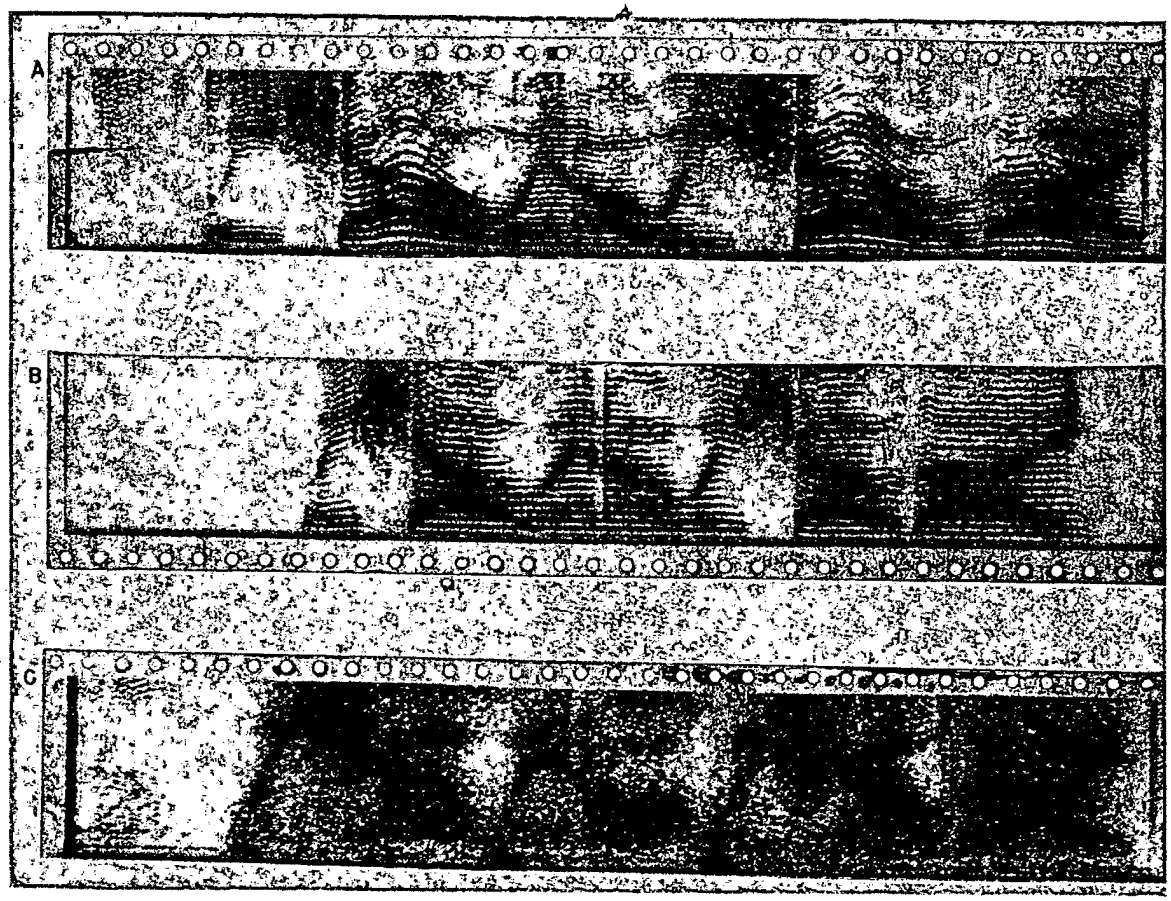



FIGURE 29. Spectrograms showing comparison of: A, normal speech; B, monotone; C, whisper.

terns which show a distinct general resemblance, but also marked differences. The speech pattern also may be considerably distorted by artificial means before the ear fails to recognize the speech, provided the distortion is not too discontinuous in frequency or time. Since privacy systems depend for their effectiveness on distorting the speech pattern beyond the possibility of recognition by the ear, it seems reasonable that this distortion would also be visible to the eye if the scrambled speech pattern could be reduced to suitable graphic form.

Examples of such patterns are shown in the attached photographs taken from the final report[44] on Project C-32. Figure 37 shows some normal speech, undistorted except that a sloping network was introduced in the electrical circuit to bring out the high-frequency structure, since this is always weaker in normal speech than the low-frequency regions. In these patterns, as before, the horizontal scale is time (about 1.8 sec is represented in each example), the vertical scale is frequency (the upper limit is 3 kc), and the density or blackness represents the intensity of the energy in a given region. It should be noted that the resolution of the process is sufficient to separate each harmonic in the voiced sounds. This is important, as will be seen later, because normally the voice fundamental is constantly changing, that is, the voice is inflected, and since the harmonics are multiples of the fundamental, the higher harmonics show progressively more change than the fundamental. For instance, if the fundamental goes from 100 to 200 cycles the tenth harmonic goes from 1,000 to 2,000 cycles, a difference of 1,000 cycles as compared to 100 cycles for the fundamental. The traces of harmonics in the

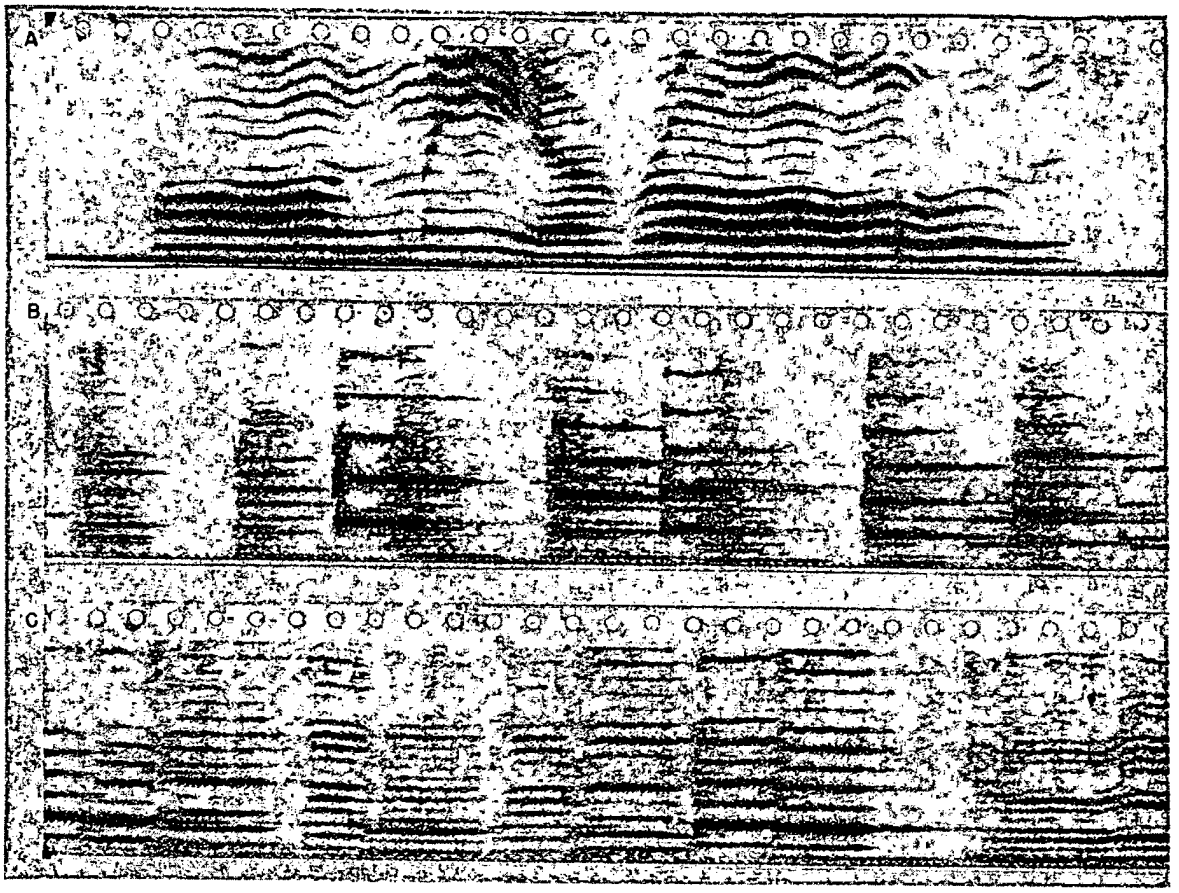



FIGURE 30. Musical effects. A, soprano voice unaccompanied; B, piano music; C, orchestra music.

visual speech patterns will, therefore, have greater slopes at the high end of the pattern than at the low end. This may be seen quite clearly in the examples of Figure 37.

Figure 38 shows patterns of some vowel sounds. In making these patterns, an attempt was made to enunciate clearly, and also to keep the pitch constant (monotone), so as to show showing transitions from one vowel to another. These pairs were chosen because their time characteristics are direct opposites.

### Scrambled Speech Patterns

Figure 40 shows the output of a privacy system which depends on simple inversion. In the inverted speech, the slopes of the harmonic

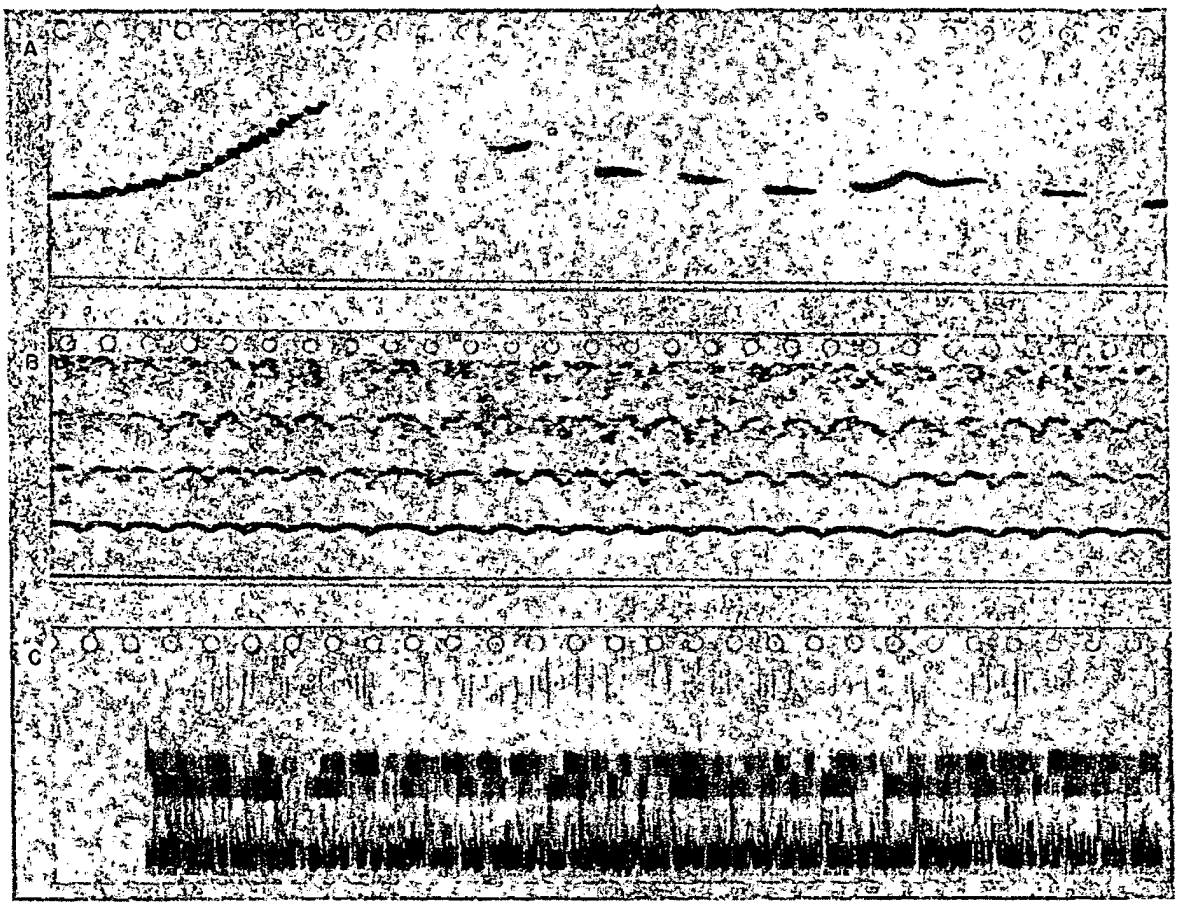



FIGURE 31. Sound effects. A, whistling with warble or rising note; B, police whistle; C, telephone bell.

the difference in energy distribution for these sounds. These are of interest because of the possibility that the visual patterns themselves might give clues as to the words they contain. Figure 38 also shows the effect on the frequency resolution of widening the band-pass scanning filter. The wide filter gives much better resolution in time, however, as will appear subsequently.

Figure 39 shows some diphthong patterns, traces become greater towards the bottom of the pattern, which is the direct opposite of normal speech, and is therefore a definite sign of inversion. The pattern also thins out at the bottom, but this could be altered by a suitable distorting network. No network, however, can change the slopes of the harmonic traces. Incidentally, the carrier "leak" shows up in the pattern, giving a direct indication of the frequency about which the inversion was per-

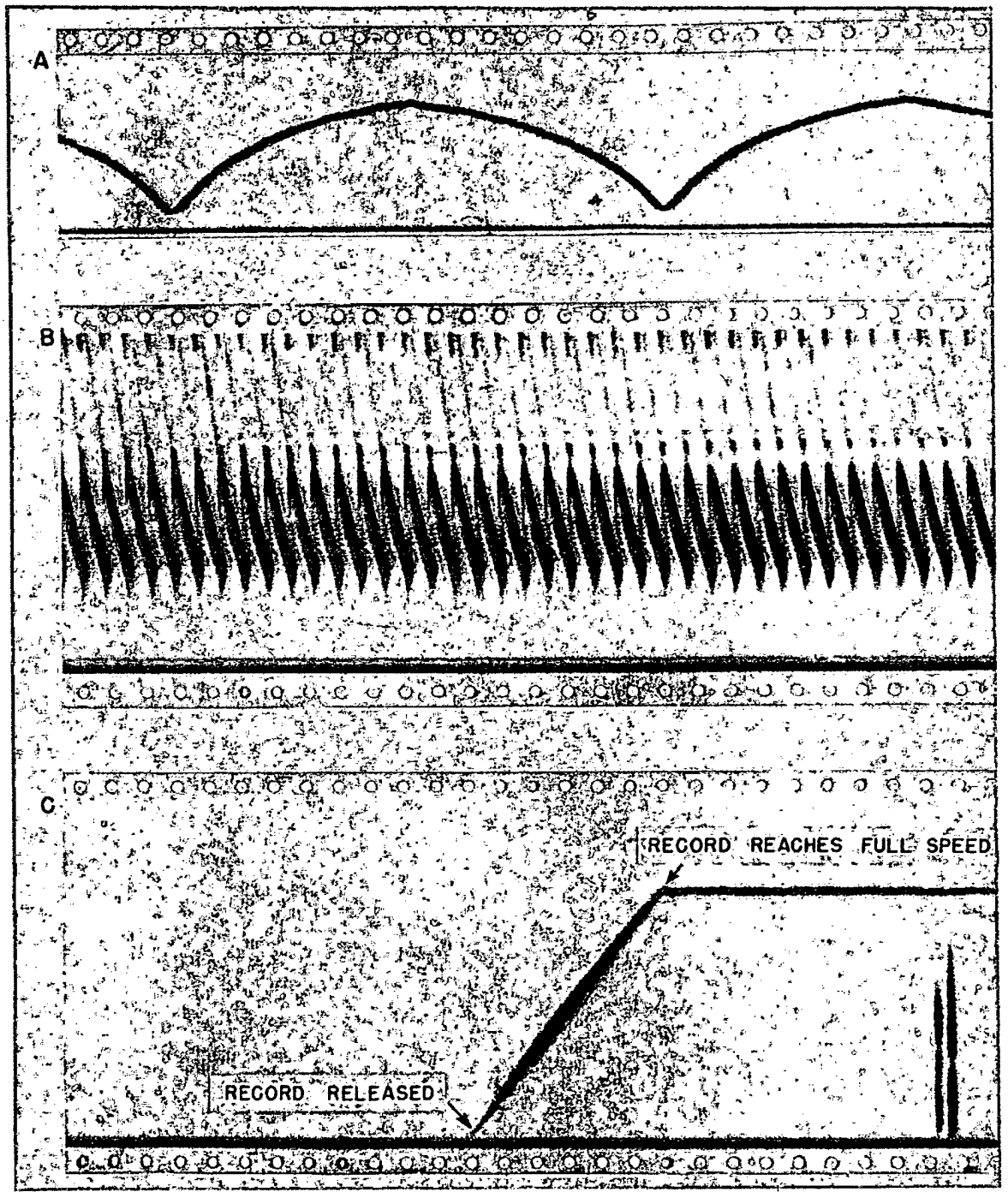



FIGURE 32. Spectrograph applications in which frequency versus time curve is presented. A, output of warbling oscillator; B, sawtooth generator output; C, acceleration of phonograph record on moving turntable.

formed. If the carrier is completely suppressed, however, its location may be determined by trial.

A more complicated privacy system is the split-band system, used in transatlantic radiotelephony, in which the frequency range is divided by filters into several bands, which are then arranged in a different order, and some are inverted. Figure 41 shows patterns of the output of such a system with two different codes. Both of these samples contain portions in which the voice was quite markedly inflected. The fact that the frequency range has been divided into five bands is quite apparent from discontinuities in the energy distribution, and also from discontinuities in the harmonic traces. It is also quite apparent that some of the bands have been inverted because the voice cannot be inflected both up and down at once. Looking at the inflected portions, it is quite easy to find one which is either definitely inverted or definitely erect. The other bands can then be immediately labeled inverted or erect depending on whether they have the same direction of curvature as the band previously identified. Now, the relative slopes of the harmonic traces in the different bands indicate their original position in the frequency scale; the band showing the least slope (or curvature) must originally have been the lowest band, and the band with the greatest slope (or curvature) must have been the top band.

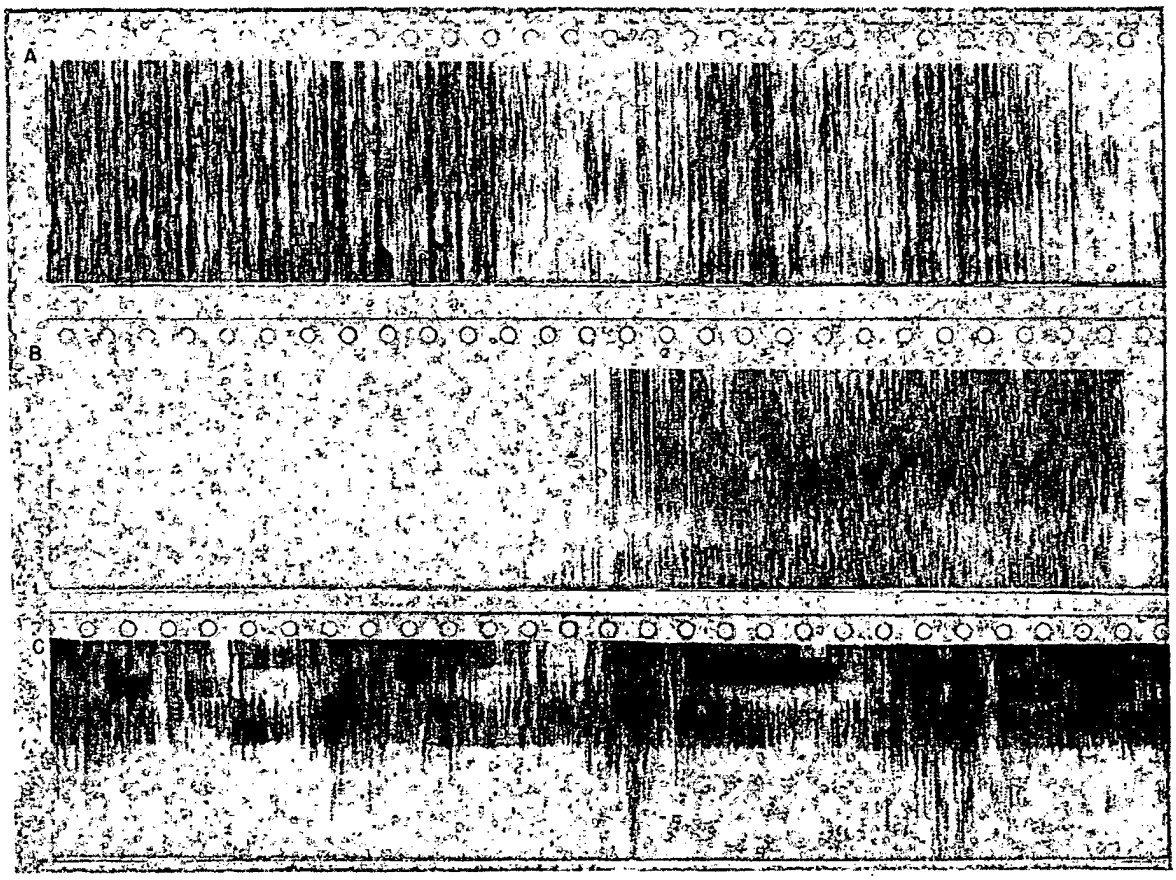



FIGURE 33. Spectrographs showing that sounds exist in high-frequency region. These are 11-kc, 1,000-cycle filter records. A, sound of crumpling paper; B, sound of tearing cloth; C, jingling keys.

The scrambling methods thus far illustrated alter the frequency characteristics of the speech patterns. The TDS privacy system, discussed in detail in Chapter 2, operates on the time characteristics of speech, dividing successive sections of speech, each $m$ seconds long, into $n$

short time elements which are sent in a scrambled time sequence. Each syllable is cut up and received as short bursts of energy in the wrong order. The number of scrambled orders available increases very rapidly with $n$. Systems have been developed in which $m$ is as short as 0.6 sec, and $n$ is 20, making each element 30 msec. A pulse of tone is sent every $m$ seconds to keep the transmitter and receiver in synchronism. In one such system over 60,000 codes are available, and they may be changed quite readily.

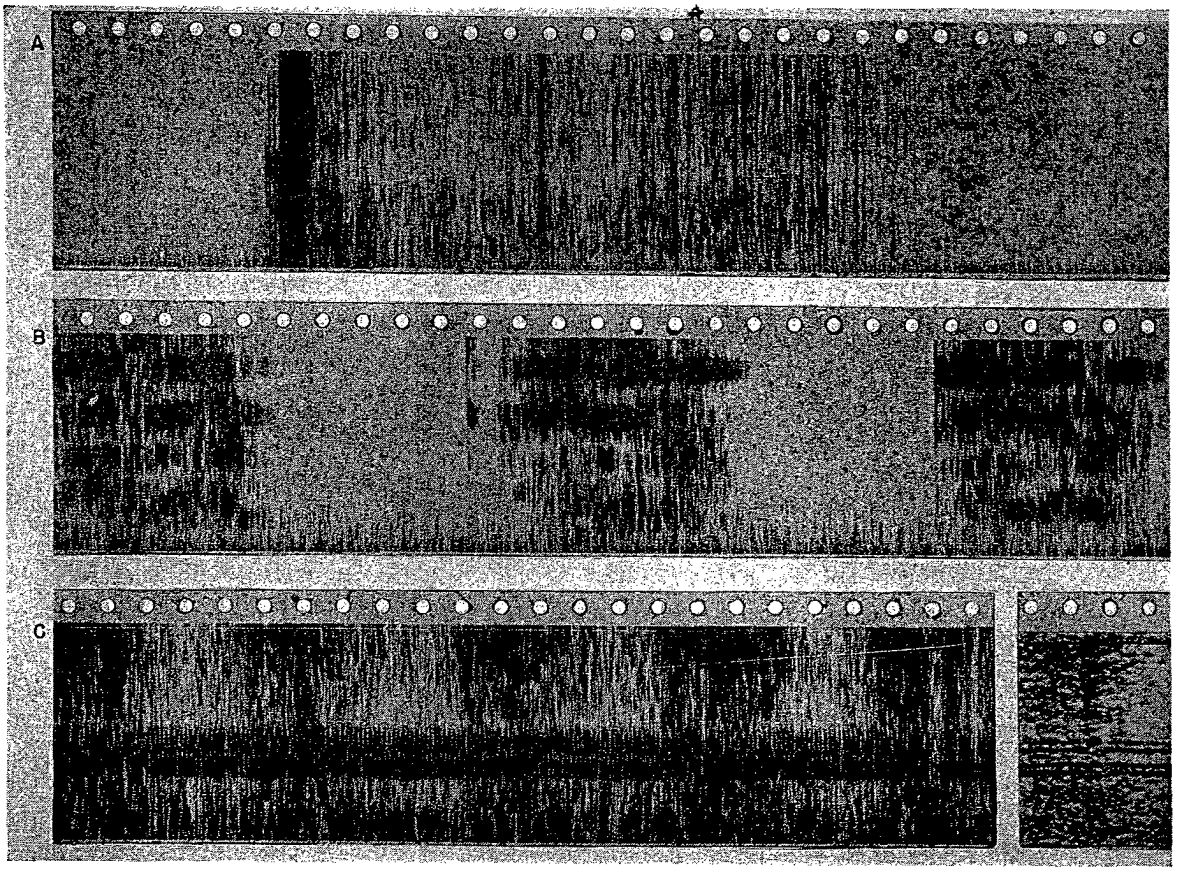



FIGURE 34. Common sounds recorded in 3.5-kc range, 300-cycle filter. A, striking match and flame; B, filing on metal; C, machinery noise; inset is same with 45-cycle filter.

## DECODING THE TDS SPEECH

Obviously, if it is desired to decode such a privacy system, it is necessary first to evaluate $m$ and $n$. Presumably a machine could be built to unscramble the speech if the code were known. Means must then be found for determining the code, and this decoding process must be repeated every time the code is changed. If the code is changed often enough, the decoding will lag far behind the message. It is essential, therefore, that every artifice be employed to increase the speed of decoding.

Figure 42 shows some speech patterns scrambled by a TDS system. It is apparent that the speech has been chopped up on the time scale rather than on the frequency scale. It is easy to determine $n$ by the length of the elements, and since the synchronizing pulse shows in the pattern, the most natural assumption is that $m$ is given by the distance between these pulses or some multiple of it. In the illustration of Figure 42, duplicate patterns were made, each element was numbered, and one of the

scrambled patterns was then cut up and reassembled, giving the code. It should be noted that in the scrambled patterns a few elements within each code cycle immediately stand out as probably belonging together, particularly when voice inflection occurs. Usually the other elements in a section cannot be positively matched. It is of tremendous help, therefore, if identical patterns are mounted on movable slides, and viewed through a system of mirrors which superposes the two, but all the upper pattern to the right of a definite line is blocked out, and all the lower pattern to the left of this line is blocked out, so that effectively any two elements may be juxtaposed to see whether they look as though they were originally con-

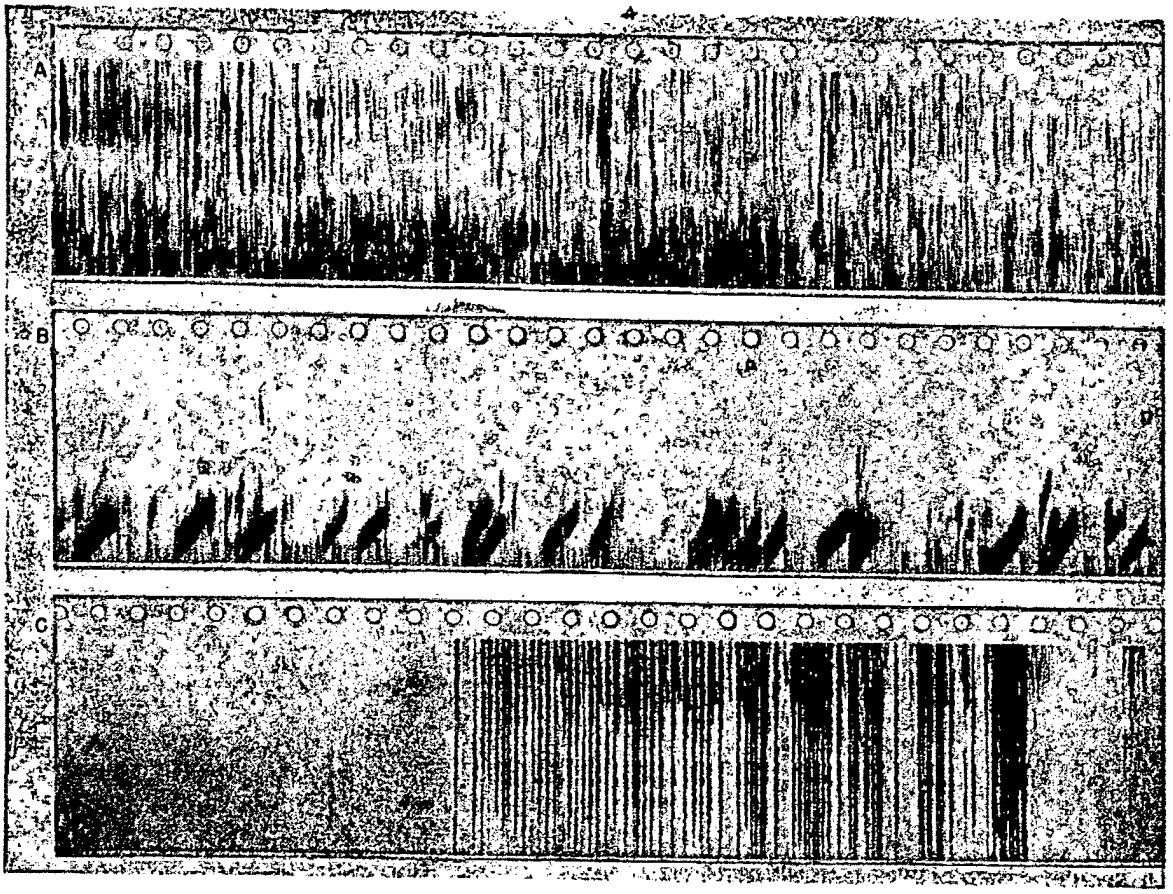



FIGURE 35. Additional 3.5-kc sounds. A, splashing stream of water; B, air bubbles blown through water; C, riffling stack of file cards.

the scrambling order is repeated over and over. A doubtful match can be checked in another section, and matches which are impossible to spot in one section can be readily spotted in another.

Rather than cut the pattern up as in the illustration, an optical system has been built for viewing two duplicate patterns simultaneously. This is shown in Figure 43. The two secutive. If a match is discovered in one section, the viewer may be shifted without moving the slides, for an immediate check in other sections. Instead of dividing the scrambled pattern with lines and numbering them as in Figure 42, suitable scales and numbers for a particular TDS system can be incorporated in the slides.

Speech patterns have been shown to be useful in decoding all systems of speech privacy known

to be in use. This method, however, which is quite general, may not necessarily be the speediest in all cases.

### Special Methods for TDS

The TDS system appears to be the most difficult to decode of all the speech privacy systems known to have been reduced to practice, particularly if a large number of codes are available and if they are changed often. A great deal of emphasis naturally was placed on TDS in Division 13 work. The following sections discuss methods particularly applicable to TDS, investigated in parallel with the speech pattern development.

*Wave Form Traces.* Speech patterns of the type thus far discussed are particularly designed to display the frequency composition of speech, so that distortion of the frequency scale could be recognized visually. Where only the time characteristics have been scrambled, the wave form itself provides evidence which can be visually interpreted. Various methods have been tried, the first being the ordinary oscillograph which discloses that there are discontinuities in time more sudden and frequent than occur in normal speech. It is possible to cut up such traces and piece them together. Examples of such records are given in the final report[44] of Project C-32.

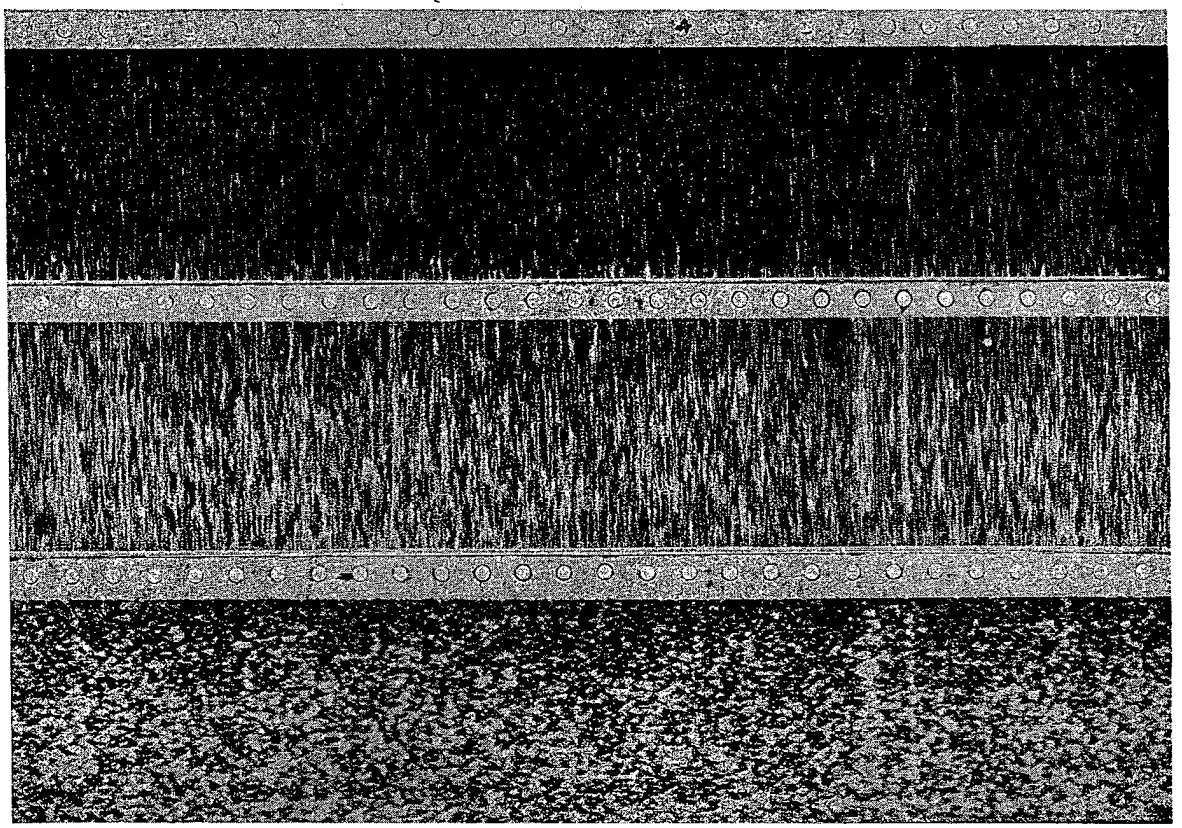


FIGURE 36. Thermal noise as example of steady sound. Two upper records made with wide filter, two levels, 12-db apart. Lower spectrograph made with narrow filter. These are 11-kc records.

It was thought that a variable-area sound track would provide more distinctive patterns than oscillographic traces, and would have the additional virtue that they could be played back, and could, therefore, serve perhaps as the primary record of the intercepted message. This scheme has proved to be useful. Examples of records made in this manner will be found in the final report on Project C-32 and in several of the preliminary reports of Project C-43.

*Partial Matching.* The above methods would not serve if the TDS code were changed very often, in the extreme case if it were changed every cycle. One branch of the investigation has, therefore, attacked TDS from a statistical

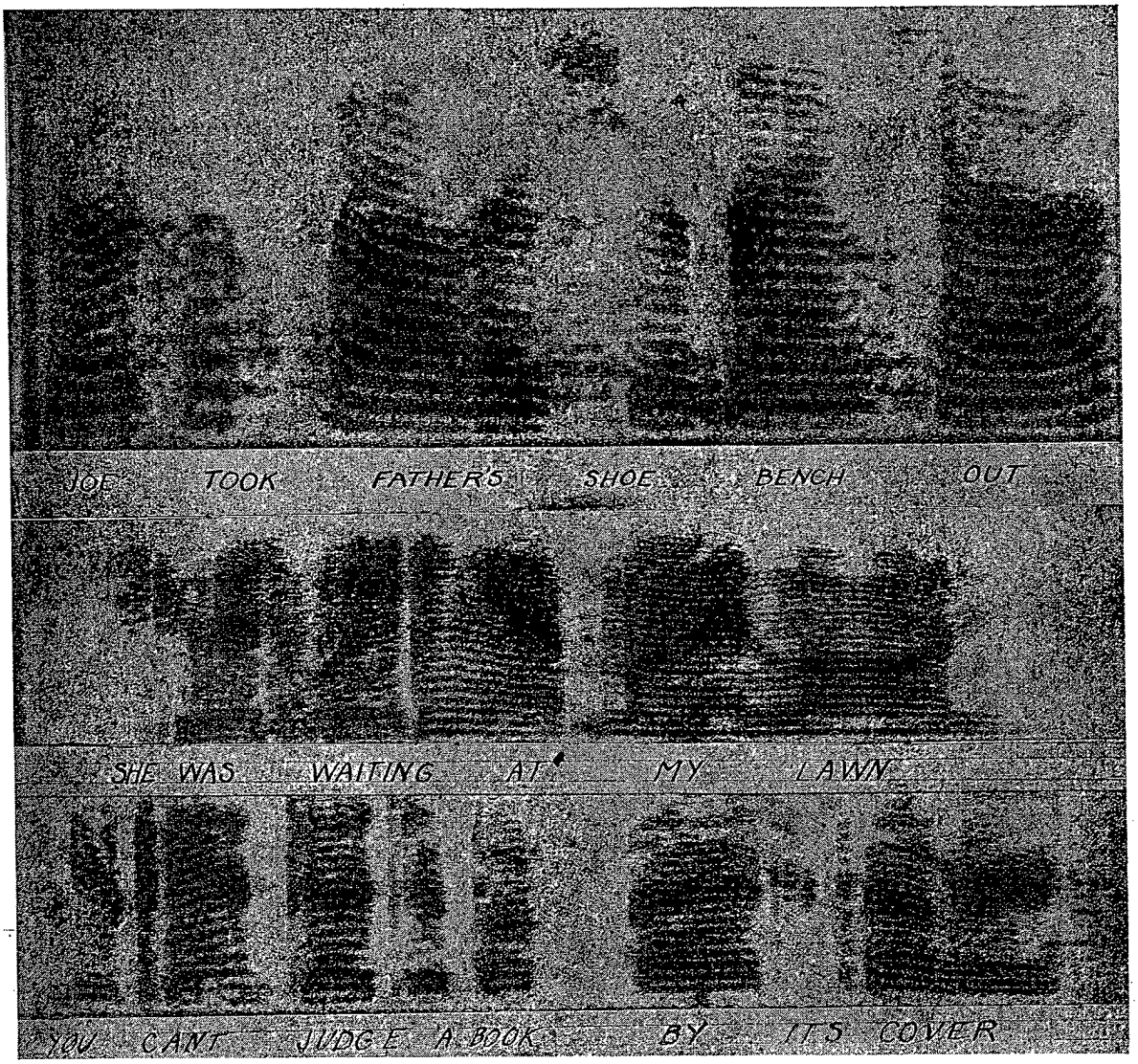



FIGURE 37. Normal undistorted speech with sloping network to bring out high-frequency structure.

angle. In a system with a sufficient number of elements the total number of available codes is very large. If, however, in a given code cycle a few elements can be visually matched, the others being inconclusive, it appears possible to tabulate in advance all the codes which will satisfy the observed matches, perhaps on International Business Machine punched cards, thereby enormously reducing the number of codes remaining possible. The most complex TDS system under consideration in Project C-32 has twenty elements per code cycle with over 60,000 good codes available. This may be reduced to only eight possible codes by matching two groups of three elements. These eight codes might conceivably be tested successively by automatic means, the correct one being recognized by ear. Presumably, the message could thus be decoded cycle by cycle. A cycle contain-

ing insufficient material for visual matching may contain no indispensable portion of the message either.

### Further Possibilities

Assuming that the methods outlined apply to all privacy systems which it is desired to crack, further work would be directed toward speeding up the processes. Improvements in speed can, it appears, be made in all of the processes outlined previously. These improvements may be summarized as follows:

*Instantaneous Speech Patterns.* With the sound spectrograph the selected sample of speech is scanned at more than twice its normal speed, the filters, etc., being designed for this purpose. It appears quite feasible, by pushing this process up into television frequencies, to obtain speech patterns of the same type on the face of a cathode-ray tube, for instance, representing either a "still" or a "moving" picture of, for example, 1 sec of speech. In the latter case the picture would be running off one edge of the screen and onto the other continuously. Desirable sections could be stopped at any time. This appears, however, to require considerable equipment as well as considerable development, and would be undertaken only if it appeared quite certain that speech patterns afforded the best means of keeping up with a rapidly changing code.

*Large Variable-Area Patterns.* The variable-area pattern method discussed above did not require photographic film, but the patterns had to be photographically enlarged for easy inspection and handling, which is a slow process at best. It does not appear impractical, particularly if it is not necessary to play the record back, and if the high frequencies are going to be modulated down, to develop a simple recording system to produce patterns of the variable-area type big enough to see and handle without enlargement, thus providing instantaneous patterns. For cases where the code is repeated, a cylinder, revolving synchronously once per code, with a corresponding lateral movement, would give a spiral record on which the similarly located elements of each code cycle would

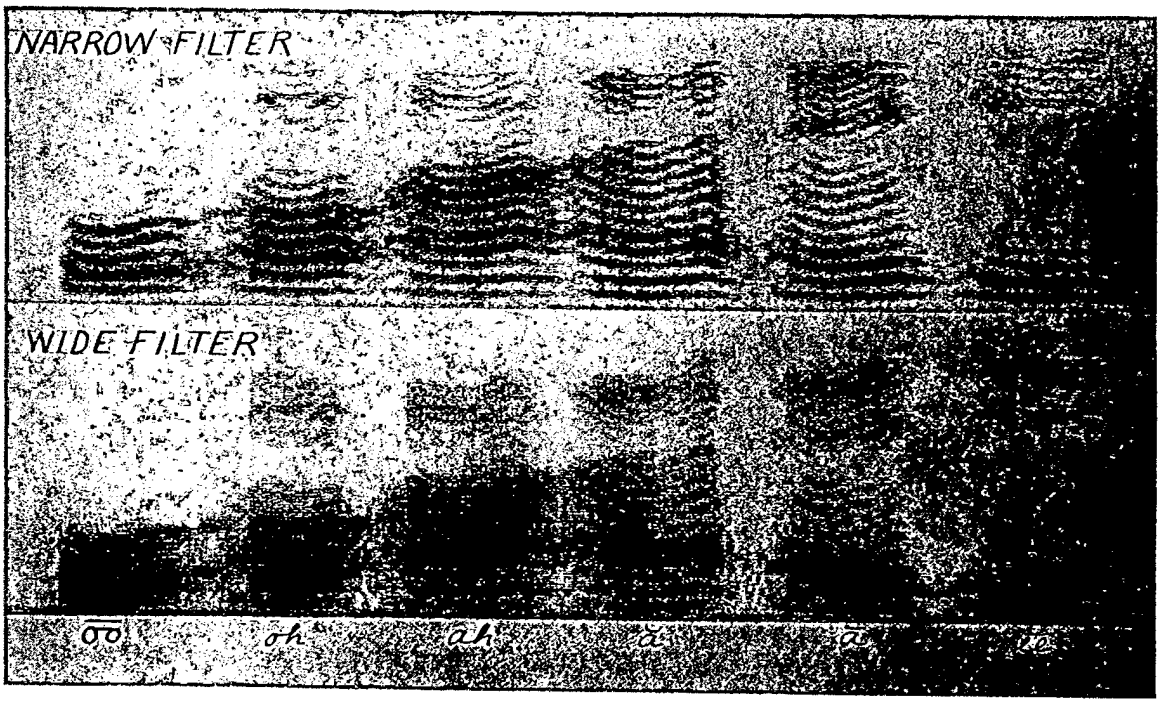



FIGURE 38. Patterns of vowel sounds showing effect of wide and narrow filters.

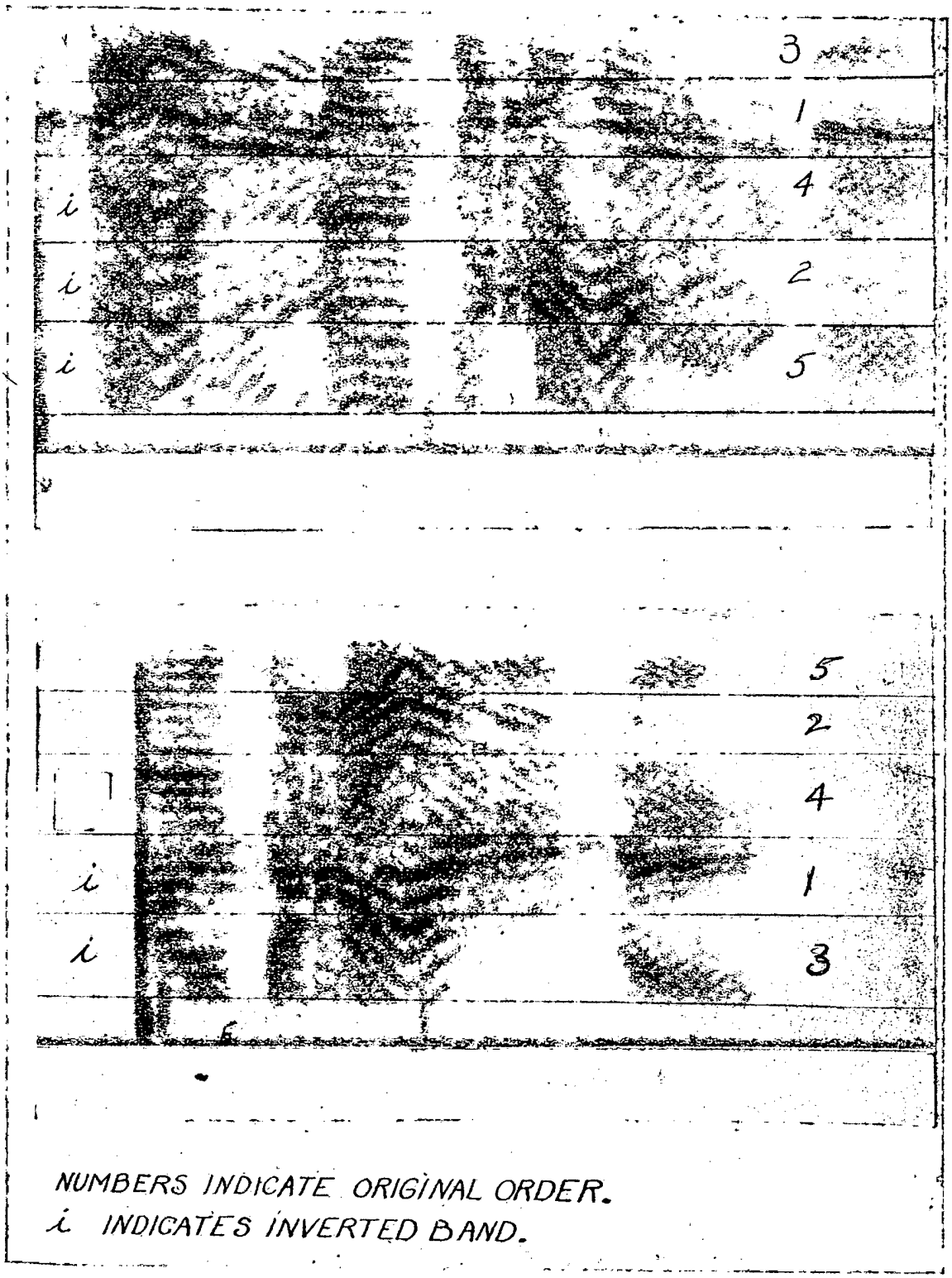



FIGURE 41. Patterns from split-band privacy system.

SECRET

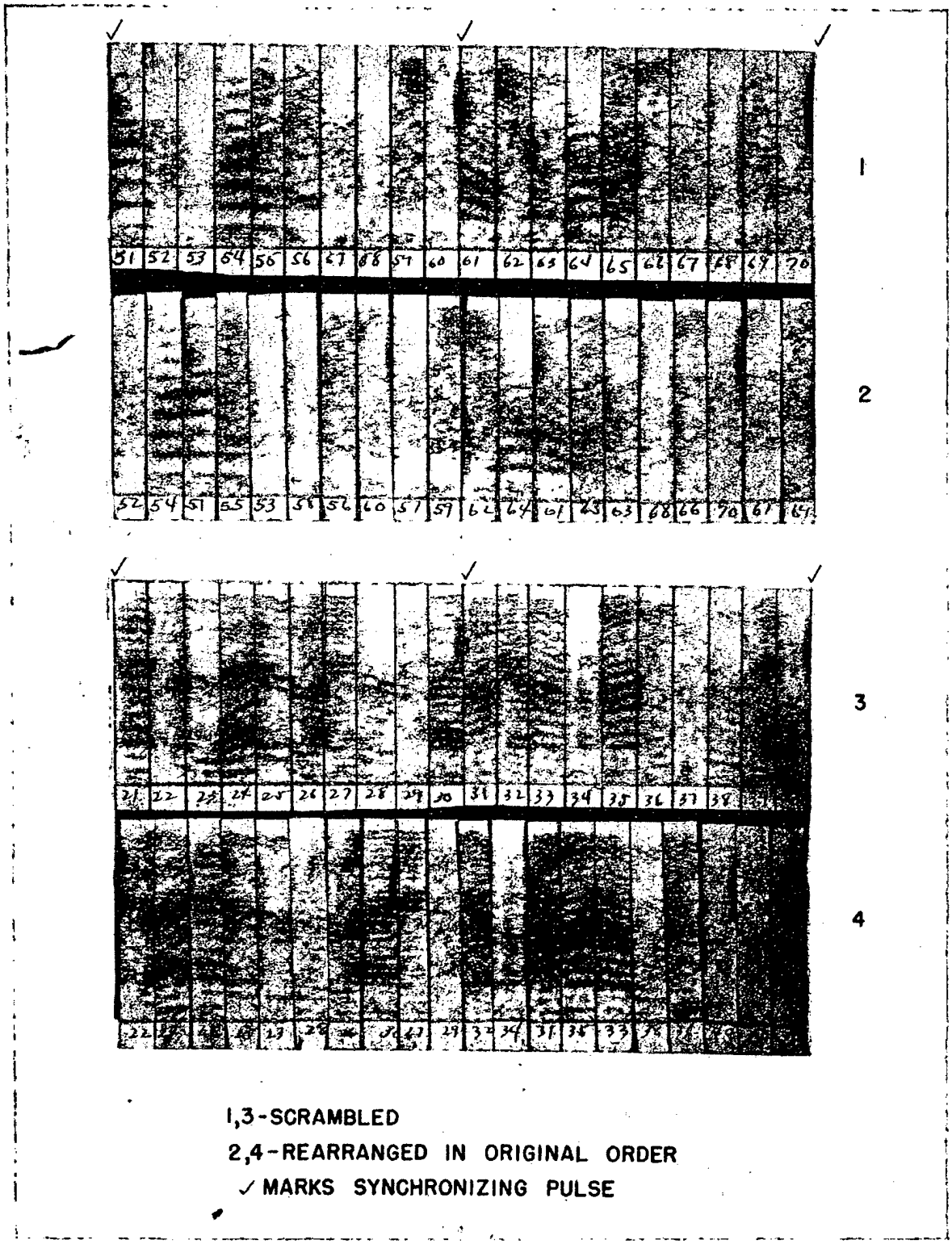



FIGURE 42. Examples of TDS speech with elements cut apart and reassembled.

SECRET

be vertically arranged so that several matches could be seen simultaneously.[17, 22-24]

*Decoding by Automatic Trial.* It appears quite feasible to combine a modified TDS receiving machine with a crossbar switch system, actuated by punched cards, perhaps, so as to try successive codes until one unscrambles the speech. This is particularly applicable to cases where the code is changed often, but where the number of possibilities can be greatly reduced by visual means. It is also applicable to cases where the total number of available codes is small.

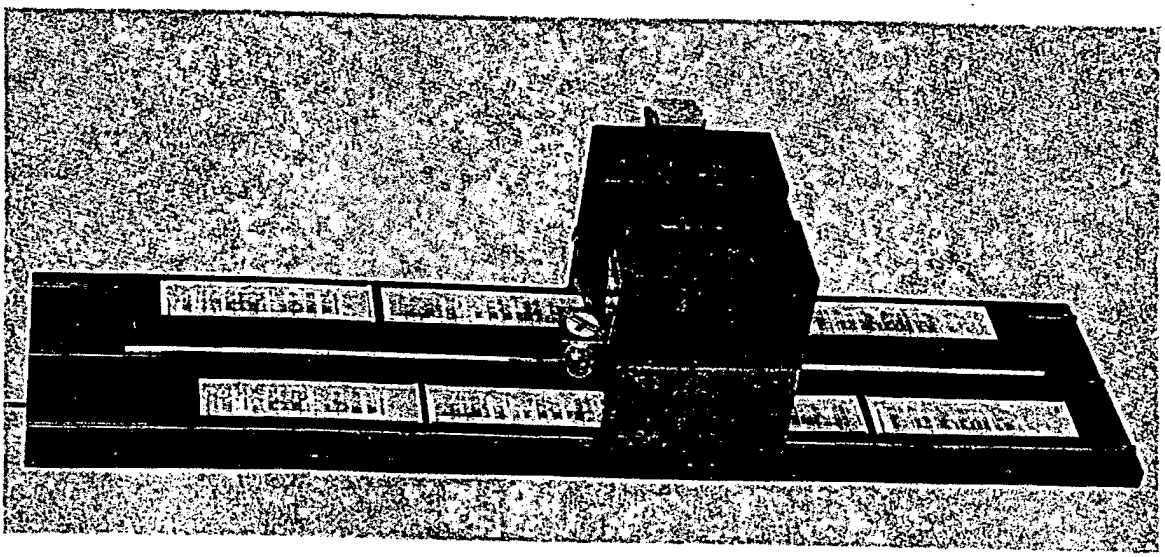


FIGURE 43. Optical system for comparing duplicate patterns simultaneously, avoiding necessity of cutting up spectrograph.

*Decoding Equipment.* Equipment might be assembled for actually decoding scrambled speech. For instance, a system of adjustable filters and carriers might be built to take care of all split-band systems. This includes shifting and inverting frequency bands, introducing different delay into various bands, removing bands of noise, wobbling the carrier, and whatever other frequency distortion may be included. A TDS decoding system with adjustable elements and codes also deserves consideration.

### 4.5.8 Additional Material in Project C-32

In actual use, the spectrograms made of records of scrambled speech are analyzed in several ways. First a visual inspection will tell whether portions of the speech are inverted or not and the discontinuities in frequency or time or pattern will reveal the coding system used at the remote transmitter. The individual segments of the spectrograph may be cut apart with shears and reassembled so that the unscrambled pattern may become evident. Having determined the nature of the scramble, equipment can be assembled or existing equipment can be adjusted so that future samples of the scrambled speech may be translated audibly as they come in.

In the final report[44] on Project C-32[a] will be found a discussion of methods for making speech patterns other than those described here, and the results of using certain foreign language records (Linguaphone) in an effort to discover if the spectrograph was universally usable without the necessity of having foreign language experts on the decoding staff. It was found that the fundamental characteristics of speech are universal and that the means by which a recorded sample of scrambled speech was distorted could be worked out even if those in charge of the equipment did not understand the language employed.

[a] Project C-32, Contract No. OEMsr-230, Western Electric Company, Inc.

## 4.6 PRACTICAL EVALUATION OF PRIVACY SYSTEMS

Experience has shown that there is a strong tendency to underestimate the security or military value of a given privacy system as soon as laboratory studies have indicated that the system can be cracked. An attempt will be made here to point out the great difference between what might be termed theoretical or laboratory evaluation and practical or field evaluation, written from the standpoint, not of the man interested in decoding a system, but of the man interested in getting a practical privacy system into use in the field.

### Cracking Time

The objective of a laboratory study of a privacy system is to obtain some kind of quantitative measure of the time or effort required to decode the system. The questions are: "How long does it take to determine the code, and how much equipment and how many people are required?" The coding and decoding processes are studied in detail, possibly with the aid of mathematical analysis, to determine whether there are any weaknesses or any characteristics of the coding process of which advantage might be taken to assist in the cracking process. Possibly a noncryptographic method will be found to apply. In this case the cracking time reduces substantially to zero. If noncryptographic methods are not applicable, available cryptographic tools and methods are brought to bear. Usually a new scrambling system will require modifications or changes in the existing tools or techniques. Possibly the basic methods can be improved for use against this particular system, or possibly new methods can be devised. Presumably after all this development work the project personnel will have become skilled in the art of decoding this particular system. The cracking time can then be determined quantitatively, perhaps with estimates as to how far this may be reduced by further skill.

In the case of repeated-code systems, the cracking time determined in the above way substantially represents the total decoding time, because, as mentioned previously, this code can be set into a receiving machine and the message obtained directly. Some additional time might be added, however, for determining what was said during the time that the code was being determined.

The procedure outlined above is very well illustrated in the series of preliminary reports on Project C-43 covering the development of cracking methods for the repeated code TDS system. They include mathematical analysis,[30, 31] the development of a new decoding tool,[22, 23] and the reduction of the decoding technique to a routine.[19] In the case of the multiplication system, the chronological steps are in one report.[27]

Too often the cracking time, as determined above, is quoted without qualification to describe the security of a system. It is, of course, usually understood that the use of this figure involves the following assumptions: (1) that the enemy knows all about the coding system, (2) that he is equipped with an adequate supply of the machines (our own models may still be far from the production stage), (3) that he has developed the same decoding tools and techniques that we have (some of our tools may be entirely new and secret), (4) that he is equipped with an adequate supply of the decoding tools, (5) that he has men trained in their use, and (6) that he is in a position to receive a good signal free of interference. Such assumptions certainly represent an extreme possibility. Experience has shown that there is a strong tendency to forget just how extreme a condition such assumptions represent. Even if the assumptions are valid there are still other factors which affect the military value of a privacy system.

### Nonrepeated Code Systems

If the code is changed periodically it may be necessary to have several decoding teams working in parallel to keep up with the transmitted material. The number of teams which will be required depends on the relation between the intervals of the code changes and the cracking time. No particular difficulty presents itself in expressing the decoding effort under these conditions in terms of man-hours. The evaluation is complicated, however, by the necessity for additional equipment, not only for decoding but for recording.

In the case of nonrepeated code systems, the cracking time for any given portion of a message will, in general, be long compared to the duration of that portion of the message. Every portion of the message must be cracked individually, and the decoding effort can be expressed as a ratio of decoding time to message time. This ratio may be 1,000 or 100,000 to 1, that is, each second of message will take 1,000 or 100,000 teams to keep up with the messages as they are spoken.

This kind of evaluation is somewhat unsatisfactory, because the length of time it will take the enemy to determine the intelligence in a particular sentence which might carry military information will depend on whether or not he is at the moment working on this sentence or whether he is wasting his time decoding previous material which might contain no information of value to him. In fact, it has been proposed that the security of such high-privacy systems could be materially enhanced by keeping the circuit 100 per cent busy with all kinds of material, possibly even from recordings, making certain that the enemy has no way of determining when the circuit is being used for passing important information. As in the case of nonrepeated code systems, it seems a bit unrealistic in evaluating such a system to assume that the enemy will seize upon the few seconds of message time which are important, and to compute the length of time it will take him to decode that portion of the message.

### Code Analysis

Many schemes have been proposed for generating ever-changing codes by a combination of short cycles geared together in such a way that the number of elements in the cycle is the product of the number of elements in the individual cycles. One scheme is to use odd ratios, such as 99 to 100, so that the code cycle will not repeat until the smaller wheel has made 100 revolutions. In other words there are 9,900 steps in the code cycle before it repeats. Another scheme is the cyclometer type in which one wheel rotates one step for each revolution of another wheel. Again the total cycle is the product of the number of steps on the individual wheels.

Such schemes should be distinguished from truly nonrepeating codes, because wherever cyclic processes are used, they are subject to analysis. This is a matter pertinent to the field of cryptanalysis and will not be discussed here. In general, it may be said that the difficulty of solving such long cycles is not determined by the total length but rather by the length of the individual subcycles.

Systems designed to produce a long code sequence usually contain provision for readjusting or realigning certain elements periodically or from day to day. Assuming that we know all about the system except the momentary settings, estimates can usually be made of the length of time and the number of people it would take to determine the unknown settings by analyzing a given sample of the code sequence. The analyst requires a knowledge of the code for a long sequence of scrambled speech before he can begin the work aimed at determining the unknown settings. He must obtain and solve a sufficiently long sample of the scramble and then analyze this sequence to obtain the settings. Too frequently the evaluation of a coding system is based on the analyzing time alone whereas the time required for solving or unscrambling a long sequence of scrambled speech may be overwhelmingly greater than the analyzing time. In fact if there is no way of solving the code sequence from the scramble alone, then the analyst can contribute nothing, and the system is still secret regardless of any inherent weakness of the cyclic coding system.

### Field Evaluation

The continuously changing military situations of modern warfare require rapid means of communication in order that the required military actions can be taken. A perfectly secure speech privacy system is of no military value if it requires so much time for encoding and decoding that it slows up the communication system to the point where appropriate steps cannot be taken when needed. Similarly, a cracking system is of no value if it is too slow to permit countermeasures to be taken according to the intercepted intelligence. For certain purposes 15 min or even 5 min cracking time

is much too slow. Where this is true, a privacy system giving 15 min or 5 min privacy is just as good as one with an hour's security. This is important because systems affording a few minutes of privacy were developed in portable form, whereas those providing longer privacy were not.

Consider also the equipment and trained personnel required for decoding intercepted communications. As a specific example, the small TDS unit required about 15 min for decoding but it required a van-load of highly specialized equipment.[32] Suppose the small portable TDS unit were used in many planes and tanks and other mobile equipment that required some privacy. Suppose also that different codes were used within different groups of units and that the codes were changed at some reasonable interval. Would it be worth the enemy's while to provide enough decoding equipment and enough trained personnel to follow these units around and decode their messages? If it is not worth his while, then units rated as low in privacy may provide high-grade privacy under such conditions.

Obviously the foregoing does not apply if the units are used to convey messages between the higher echelons of command. In such cases the messages have a longer term significance to the enemy, and he can afford to devote considerable time and equipment to intercepting and decoding them.

Advantage might also be taken of the element of surprise. Suppose we suddenly introduce in the field a low-grade privacy system in large quantities. How long would it take before the enemy diagnosed the system, developed a decoding method, manufactured receiving sets of the proper type and also decoding equipment, distributed these where needed and organized and trained personnel to use them? Until he has done these things the units provide complete secrecy. A different kind of system might then be introduced which would again provide secrecy for a time.

It is intended simply to point out that there are other considerations in the evaluation of privacy systems than the time it takes a highly specialized group, such as the personnel of Project C-43, to decode the system under the ideal conditions of a laboratory. The decoding time alone is often quoted, because it is the only element which can be described quantitatively. While there is always theoretical agreement about the existence of the other considerations, they cannot be pointed out too often or too strongly.

## 4.7 DIAGNOSIS OF UNKNOWN SYSTEMS

Before discussing the diagnosis of speech privacy systems it should be pointed out that facts concerning the origin of unknown signals are often very necessary to their correct interpretation. Such things as the frequency, strength, and direction of the signals, the location and type of receiver, and the manner in which the signals were recorded, can be very important data. That is why interceptors should be equipped with complete knowledge of the various kinds of radio systems and transmissions used by both sides, including jamming and radar signals as well as telegraph and facsimile signals. Some of these signals, particularly if transmitted with suppressed carrier, can give extremely puzzling results if demodulated with an ordinary radio set. These possibilities should be taken into account if signals are found which do not seem to fit into the classes discussed below.

As stated before, the spectrograph is of tremendous assistance in recognizing the nature of an unknown scrambling system. The ear can usually recognize the presence of time discontinuities. It can also usually recognize the peculiar quality which results from band-shifting systems. The exact nature of the scramble, however, is usually impossible to establish with the ear. Even scrutiny of the wave form may yield no clue. The strikingly graphic analysis provided by the spectrograph, however, usually takes the mystery out of the scrambling method immediately.

Speech privacy systems having frequency subbands will show horizontal discontinuities or boundaries in their spectrograms. Similarly systems employing time division will show vertical boundaries. A considerable variety of systems display both horizontal and vertical bound-

aries. How to tell these different scrambling systems apart is the subject of the discussion and illustrations to follow.

## Measurements on Spectrograms

Since an important part of the diagnosis procedure consists in determining the length of time elements and the location of frequency boundaries, let us first examine the procedures whereby the time and frequency scales of the spectrograph can be established. The spectrograph is equipped with a calibrating device which consists of means for producing a complex wave rich in harmonics from the 60-cycle power supply. Spectrograms of this wave made with both the 45-cycle filter and the 300-cycle filter are shown in Figure 44. If the power frequency is known, the horizontal and vertical striations in these patterns provide the time and frequency scales. If the power frequency is not known the scales may be established by the formulas given in the figure. This involves additional measurements with a stop watch.

The application of this method to 11-kc spectrograms is not explicitly stated in the figure. A value of $K$ for this condition can be found by the same formulas. This establishes the time scale for the 11-kc spectrograms. For the frequency scale the same pattern is used as for the 3.5-kc spectrograms. However, each horizontal striation is labeled with a frequency obtained by multiplying the normal frequencies by the ratio of the two $K$'s.

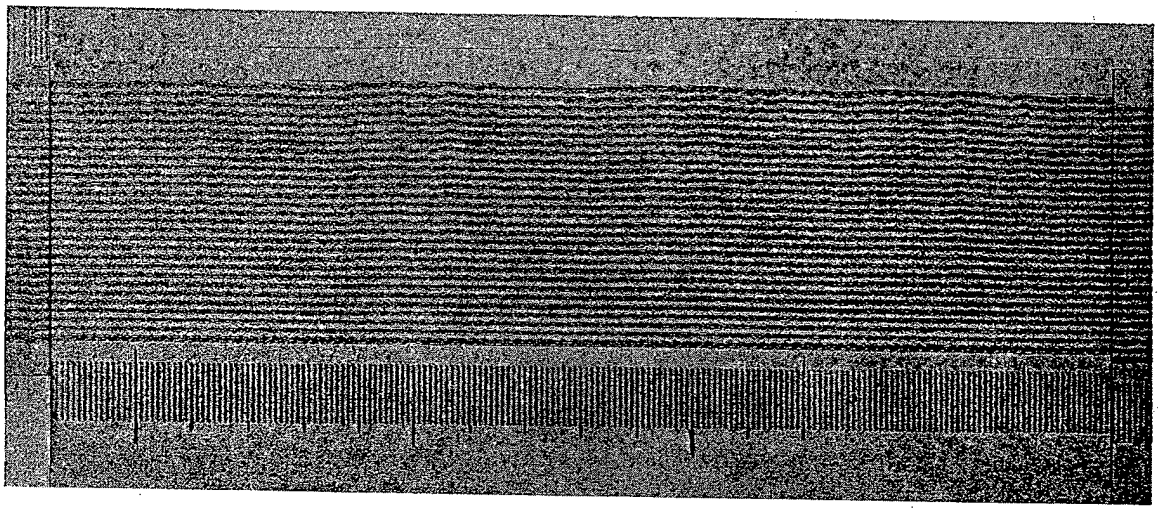


FIGURE 44. Calibration of spectrograph scales.

The upper spectrogram (narrow filter) shows all the odd harmonics of the 60-cycle input to a special harmonic generator. In the wide filter spectrogram (below) the striations represent a beat note of 120 cycles.

At the left is a portion cut off and inverted. The fact that the harmonics can be lined up in this as well as other shifted positions illustrates the linearity of the frequency scale. At the right is a portion cut off and shifted downward by one component. Since the harmonics are *odd*, the base line will fall exactly between two harmonics if it represents exactly zero frequency.

If the power frequency is exactly known, both the time scale and the frequency scale are determined by the two patterns above. If the power frequency is not known, the time scale factor can be determined by the equation $K = LR/T$ inches per second, and the frequency by $F = KS/N$.

$L$ = Total length of the spectrogram (circumference of the recording drum).

$R$ = Number of rotations of the drum in $T$ seconds.

$S$ = Number of striations in $N$ inches.

Figure 45 shows how these scales can be used to measure the time and frequency boundaries in a scramble. It will be noted that for measuring the time elements spectrograms made with the 300-cycle filter are best because they have sharper time boundaries. For measuring frequency boundaries the same filter must be used as was used in obtaining the scale. It may be noted here that in present models of the spectrograph, the wide filter has a different absolute location than the narrow filter and therefore should not be used to estimate the frequency of components or boundaries.

### Illustrations of Scrambled Speech

Spectrograms illustrating a large number of privacy system scrambles are shown in Figures 46 through 65. In so far as possible, these spectrograms were obtained with actual working models or systems. In some cases they were made with a laboratory setup simulating the systems under scrutiny. In a few cases also the illustrations were made by cutting up spectrograms and rearranging the parts. It should be noted in these latter cases that the boundaries are unnaturally clear and sharp because in practice any discontinuity causes a transient which tends to obscure the true speech along the boundaries.

It will be noted that some of the spectrograms in the illustrations were made with the 45-cycle filter and some with the 300-cycle filter depending on what features were to be brought out most clearly.

In some cases the spectrograms alone are not sufficient to determine the exact nature of the scramble. Certain systems completely destroy the typical harmonic structure of speech leaving structureless patterns which cannot be interpreted. This indicates a distortion of the wave form. One of these systems, which had a repeating code and a synchronizing pulse, could be resolved by the method shown in Figure 55.

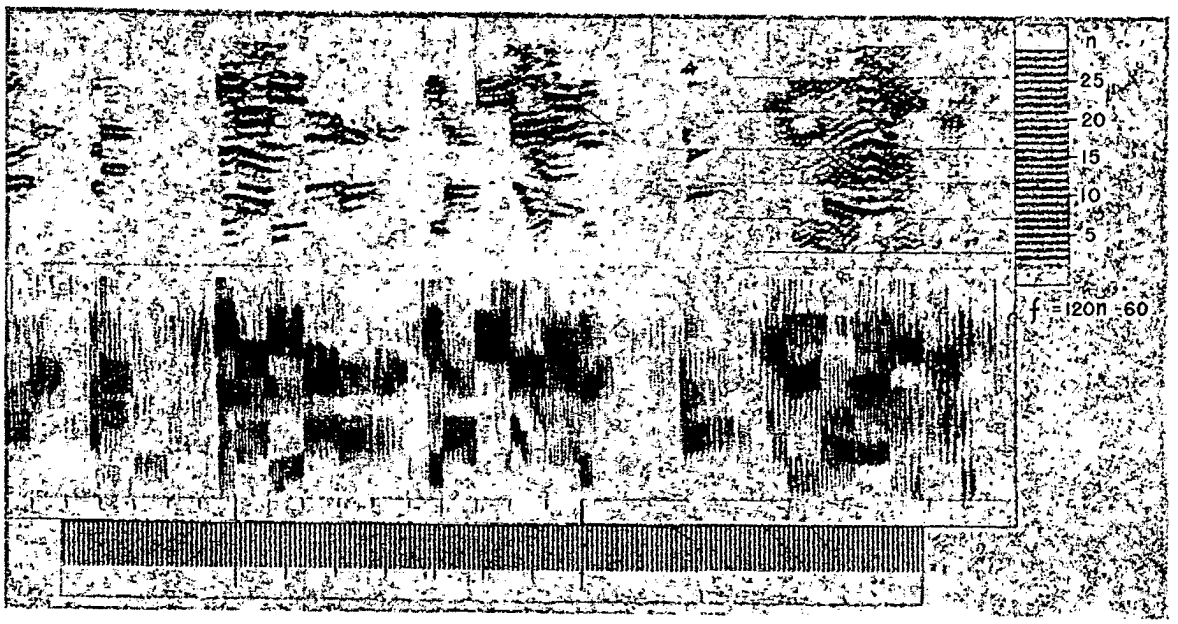



FIGURE 45. Time and frequency measurements.

Upper spectrogram, 45-cycle filter; lower spectrogram, 300-cycle filter. The frequency boundaries are determined by comparing them with the harmonics of the calibrating wave. These are all 120 cycles apart, but the lowest is only 60 cycles from the base line.

The element length is best determined by using the 300-cycle filter which gives sharp time boundaries, comparing them with the striations obtained by making a spectrogram of the calibrating wave with the 300-cycle filter. Each one represents $\frac{1}{120}$ second. Ten of the above elements cover 70 striations. The length of each element is $\frac{1}{10} \times \frac{70}{120}$ second.

No general rules, however, can be given for diagnosing this type of system.

### Systems not Illustrated

Examination of Table 1 shows that there are a few scrambling systems which are not represented in the illustrations. These will be discussed in the following paragraphs. In most cases, the appearance of the spectrogram pattern which would result can be visualized by analogy with other systems.

The phase-reversal system (A4) will produce a scramble indistinguishable from the multiplication system (H1) provided the phase reversals occur at irregular intervals and about as rapidly as the crossovers in the coding wave

involved in H1. It is probable that they would have to occur about that often to make speech unintelligible.

The split-phase system (A5) involving carriers 90 degrees apart was tried out in the laboratory. The output appears just as if two speech channels, or a speech channel and an interfering noise, were simply superposed and then modulated with a single carrier.

The stepped displacement system (B2) is rather easy to visualize. There will be time boundaries, with two or more discrete conditions of displacement. Obviously, there are a great number of possible sequences, including the possibility of some of the conditions consisting of inverted displacement.

The irregular wobbled displacement (B4) will be similar to B3 except that the wobble pattern will not be as simple.

The continuously varied re-entrant displacement (C2) is practically impossible to simulate artificially, as was done with C1. If C1 is thoroughly understood, however, the appearance of a wobbled instead of stepped re-entrant condition is not difficult to visualize.

Nonrepeated-code TDS (F3) will have the same general appearance as repeated-code TDS. It may or may not have the synchronizing pulse. There will of course be no regularity in the patterns such as was pointed out in F2.

The spectrogram for TDS plus inversion (G1) is not difficult to visualize. Some or all of the elements might be inverted, as in A3.

The systems listed in both G5 and G6 will show equally spaced time boundaries corresponding to the length of the elements. In G5, the harmonics would be spaced much farther apart than in normal speech, and show greater slopes and curvatures. Alternate elements would show rather consistent differences in frequency distribution and in the degree of slope or curvature. In G6, the harmonics would be spaced abnormally closely, and show very little slope or curvature. Words and spaces would be very long. There would be a horizontal boundary in the middle of the band, and the patterns in each half would appear like complete spectrograms, with vowel and consonant structures apparent. In both of these systems, if the elements were cut apart, they could be rearranged to form continuous speech with the time and frequency scales compressed or expanded from the normal condition.

Level modulations (H2 and H3) would hardly show up in spectrograms because of the level compression incorporated in the spectrograph. This has been verified experimentally.

In J1 and J2, if the noise were sufficient to mask the speech effectively, the speech could not be seen in spectrograms. Patterns for J3 and J4 are easy to visualize. If the noise spurts are sufficiently close together, however, they may produce a pattern like H1. As far as is known, J5 exists only on paper.

In Vocoder types of scrambling systems the spectrograph would show only the channel signals, which might be either amplitude or frequency modulated. For this type of scramble, oscillograms of the wave form of each separate channel signal provide the best means for diagnosis and for decoding. A sample of such oscillograms, which was obtained from an actual Vocoder system, is shown in Figure 50. The various methods of scrambling such signals (K1, K2, K3, K4) will produce discontinuities in these traces which are easy to visualize. A sample of K5 has not been available.

Channel mixing (L3) can be done in various ways and at various speeds. It will not be easy to recognize if done rapidly. No actual systems are in use, as far as is known.

It is felt that the above illustrations and discussions cover the known scrambling methods fairly thoroughly. It is hoped that with their help any system which might be encountered in the future can be recognized. Certain additional spectrographic material appearing in Part I of the final report on Project C-43[b] is useful to anyone wanting all possible data on the subject. Part II[33] includes all the preliminary reports dealing with specific phases of the work carried out under the project.

[b] Project C-43, Contract OEMsr-435, Western Electric Company, Inc.

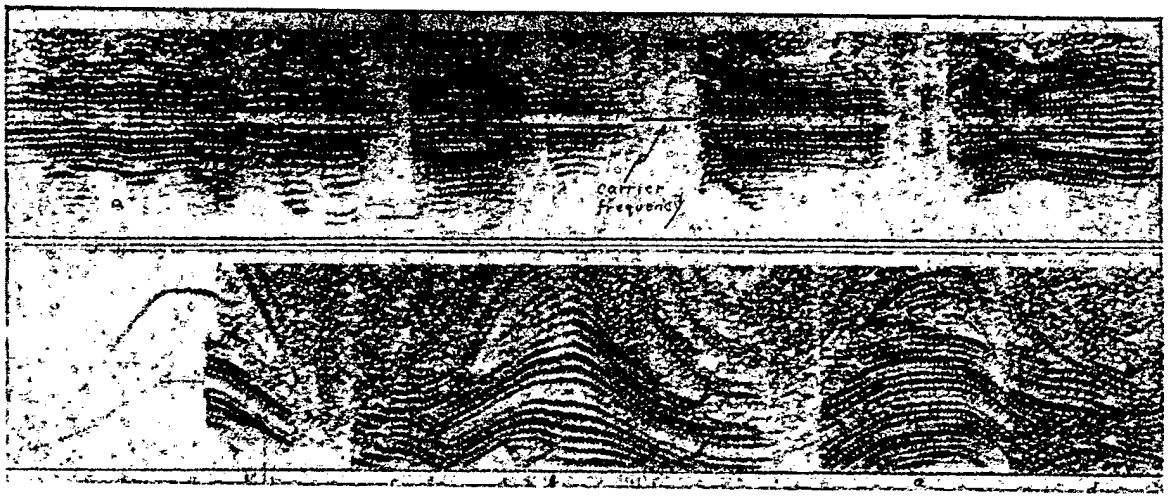



FIGURE 46. Illustrating modulation sidebands.

The upper spectrogram shows speech modulated with a carrier of 2,000 cycles. Note the symmetry of the pattern around this frequency. Each harmonic, and each resonance area, is duplicated on both sides of the carrier. This clearly shows that the two sidebands are exactly alike, except that one is inverted. The recording from which these spectrograms were taken has somewhat attenuated the frequencies near the base line.

The carrier itself is largely suppressed by the double balanced modulator; high level sounds, however, occasionally unbalance it sufficiently for the carrier to show through.

In the lower spectrogram, the carrier frequency has been wobbled at a rather slow rate. Note that as the sidebands move up and down with the carrier, the harmonics remain parallel, as at point *a*, except when marked voice inflections occur, as at point *b*.

In the clear space at the left, the wobbling carrier can be seen, together with its second harmonic. In the upper part of the spectrogram at point *a*, the second harmonic of the carrier can also be seen, with its own set of sidebands.

When the carrier frequency is low, as at points *c* and *d*, the lower sideband can be seen folding back; the folded back portion is right side up and overlaps the regular sidebands.

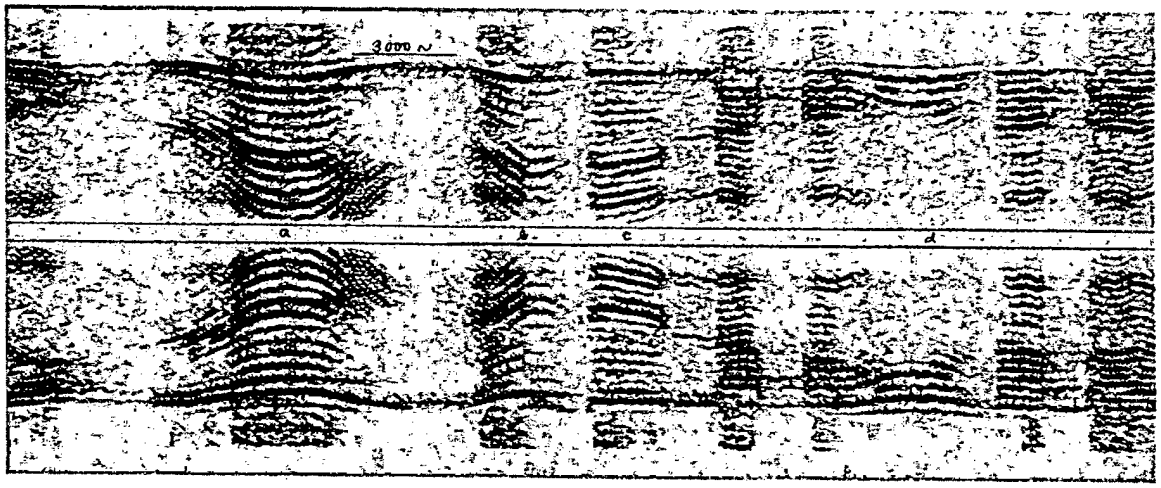



FIGURE 47. Simple inversion.

The upper spectrogram was made in the normal manner, showing inverted speech; the lower one was made with reversed oscillator sweep, producing a mechanically inverted spectrogram in which the speech appears right side up.

This sample contains harmonics with marked curvatures. These are voice inflections, and their occurrence can easily be recognized by ear. In general, samples with such voice inflections should be captured because they are most useful for diagnosing scrambling systems.

In the upper spectrogram, at points *a* and *d*, note how the curvature of the harmonics is least at the highest frequencies and progressively greater toward the lowest frequencies. Similarly, at points *b* and *c*, the slopes of the harmonics are least at the top and greatest at the bottom of the spectrogram. This is directly the reverse of normal speech and definitely indicates inversion. The lower spectrogram illustrates the normal slopes and curvatures.

There is obviously a low-pass filter in the system, at about 3,000 cycles, as indicated by the rather abrupt change in intensity. Such a filter is normally used to cut off the upper sideband. It is usually also designed to cut off the carrier. In this case, its cutoff frequency is lower than the carrier frequency. This shows up at points *a* and *b* in the harmonics, fading out before they completely flatten out. However, the inversion frequency is not far from 3,000 cycles, because the slopes are substantially zero as they approach this frequency.

SECRET

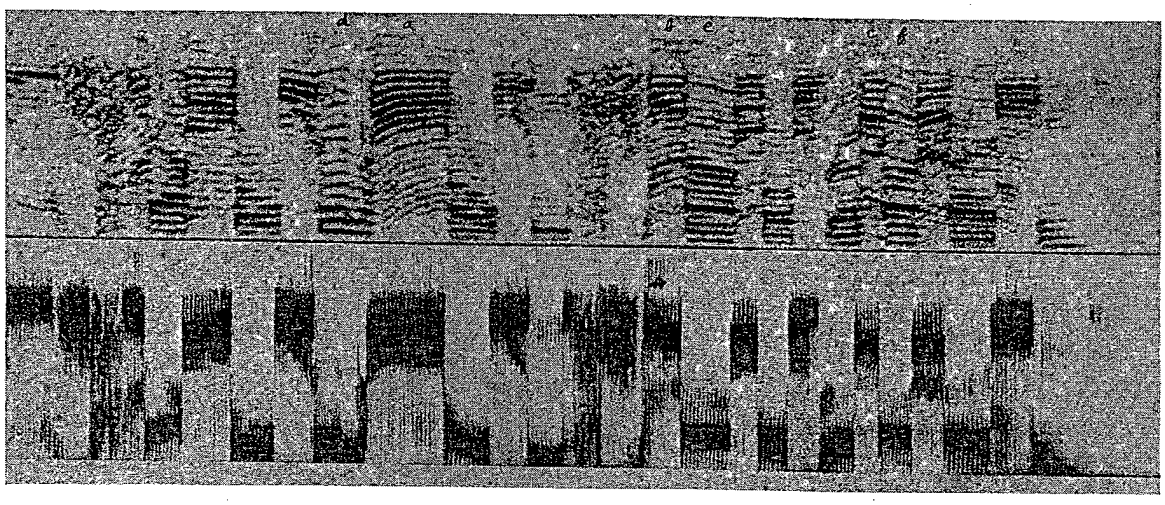


FIGURE 48. Alternate inversion.

Here the speech is divided up into sections by sharp vertical boundaries. When the individual elements are examined, *a*, *b*, and *c* show unmistakable signs of inversion. Elements *d*, *e*, and *f* are definitely not inverted.

The regularity of the dark areas in the lower spectrogram suggests that only two conditions are involved. Note also that in general, where slopes can be clearly discerned, the harmonics slope in opposite directions in adjacent elements. These indications point to alternate straight and inverted transmission.

This diagnosis could be confirmed by making a mechanically inverted spectrogram and matching together alternate pieces from the two spectrograms.

The switching intervals are irregular, with no repetition apparent within the time covered by this spectrogram. Additional spectrograms, covering a longer period, might show a repeated cycle.

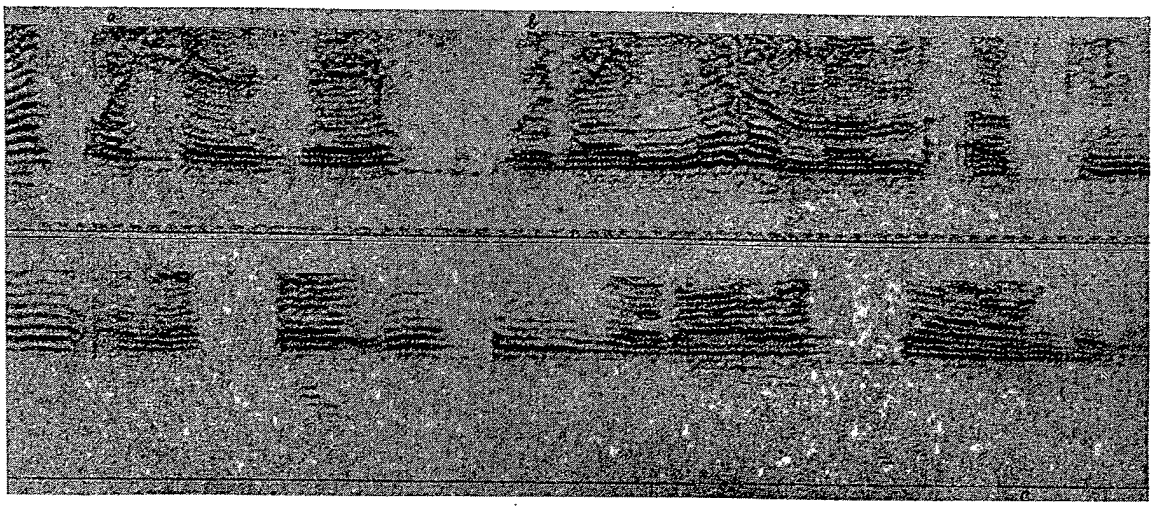


FIGURE 49. Fixed displacement.

In the upper spectrogram, the speech band has been displaced from its normal location by 1,000 cycles; in the lower one, by 2,000 cycles. Recognition of this condition is aided by familiarity with the appearance of normal speech in spectrograms. All vowels have characteristic resonant areas close to what would be the base line (zero frequency) in normal speech, and the glides such as occur at *a* and *b* tend to start from this region.

At *c*, the harmonics look as though they could meet at a point if extended to the right. This point would be the true base line.

A displacement of this type could be produced by modulating with a carrier of 1,000 or 2,000 cycles, and suppressing the lower (inverted) sideband with a high-pass filter. In practice, however, a double modulation process is used, because the displacement may be changed at will without changing the filter cutoff.

In both spectrograms, a small amount of lower sideband can be seen. This incompletely suppressed sideband would look the same whether produced by single or double modulation.

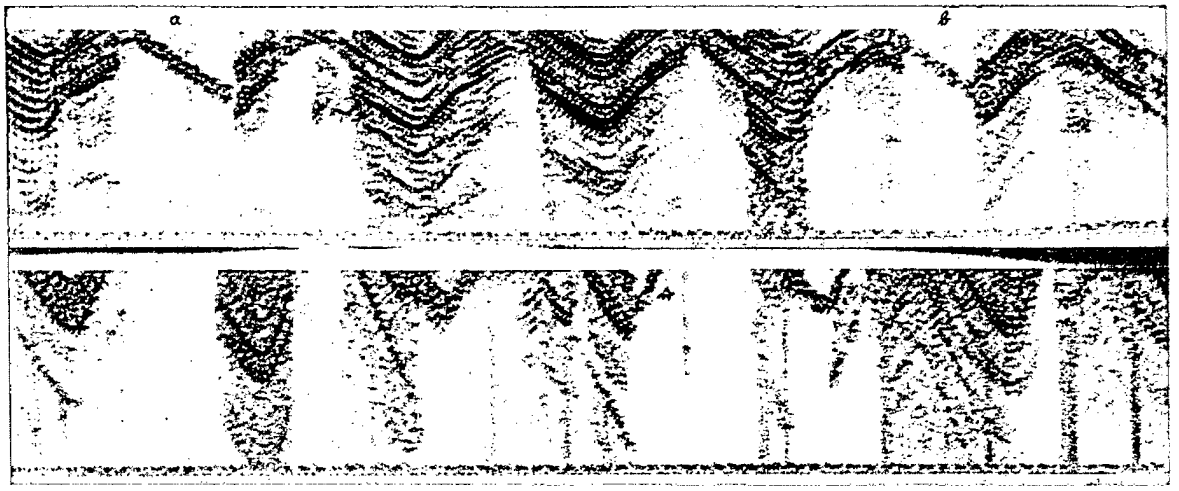



FIGURE 50. Wobbled displacement.

The upper spectrogram shows an example of wobbled inversion. Note the occurrence of harmonics symmetrically disposed about a suppressed carrier frequency which is varying between 2,500 and 3,500 cycles. Note how the harmonics remain essentially parallel. At points *a* and *b* the sidebands appear to consist only of low-frequency noise. The carrier wobble is irregular in shape but regularly repeated in time.

If there is a low-pass filter in the system, its cutoff frequency is higher than 3,500 cycles. Note that if it were lower, it would occasionally cut off some of the wanted (lower) sideband.

The lower spectrogram shows a wobble covering a much wider frequency range. The lower sideband dips below the 3,500-cycle range of the spectrogram only part of the time. This would certainly be diagnosed as a band displacement system involving double modulation. If it were encountered in practice, wide-band spectrograms would be used to determine the exact displacement.

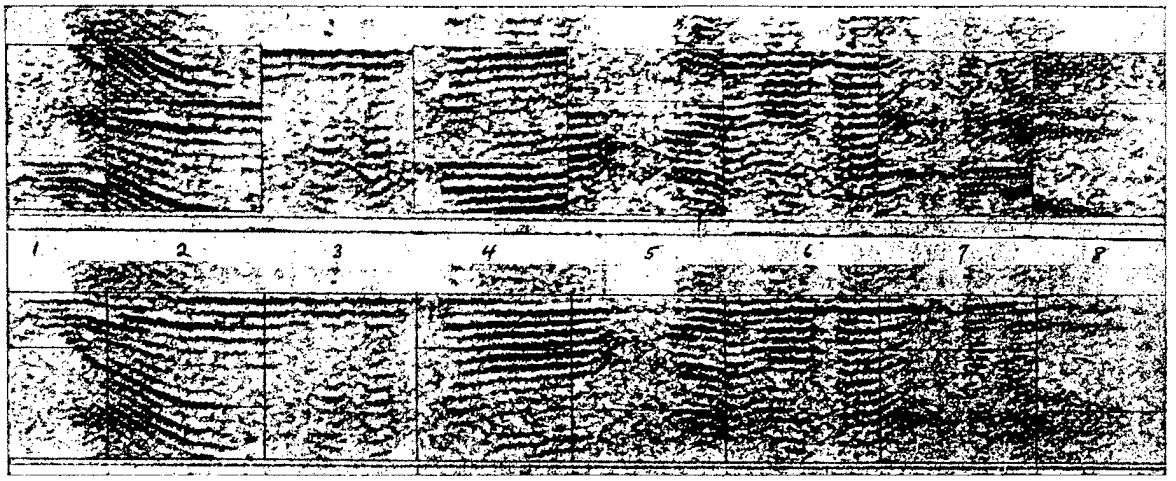



FIGURE 51. Re-entrant inversion.

The upper spectrogram was artificially produced by cutting up and rearranging a spectrogram of simple inversion.

There are vertical boundaries about 275 msec apart. There are also horizontal boundaries, but these are not continuous.

Elements 3 and 6 show no horizontal boundaries, but they show the signs of simple inversion. All the other elements show horizontal boundaries, with higher slopes above the boundary than below. If the two portions of each element were interchanged, the slopes would be in the correct order (for inverted speech).

It can also be seen that if the elements were thus rearranged, the harmonics of each element would match those of the preceding and following elements. This, of course, should be confirmed in practice by trial.

These configurations would be produced by re-entrant inversion. In terms of these spectrograms, this process results in inverting successive elements about frequencies of 1,000, 2,000, and 3,000 cycles, respectively, removing the upper sideband, and replacing it with that portion of the lower sideband extending below about 200 cycles.

The lower spectrogram is a duplicate of the one above. The boundaries have been marked off to show that the elements rearranged, as suggested above, would form continuous inverted speech.

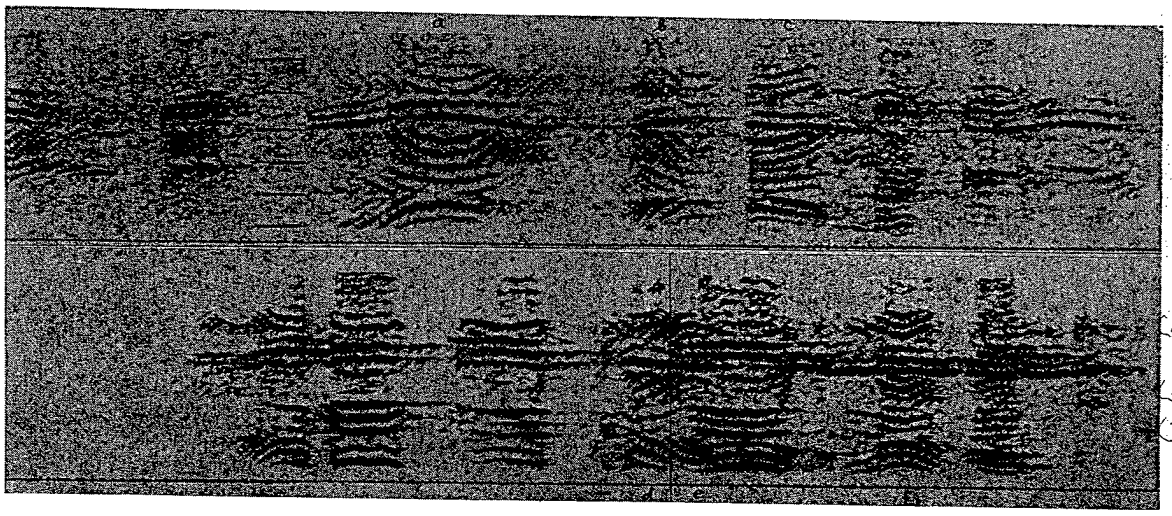


FIGURE 52. Fixed split-band scramble.

These are two samples with the same code. Note the horizontal discontinuities in the frequency distribution of energy, which can best be seen by looking endwise along the patterns. These are the filter boundaries. This system shows five bands, covering the range from 250 to 3,000 cycles. In split-band systems, the subbands are generally equally wide, for practical reasons.

There are no vertical discontinuities, other than the normal sequence of words and spaces.

Note that the harmonics slope or curve in opposite directions within a word or syllable. This indicates that some of the subbands have been inverted. The first and fourth bands are clearly normal, the others are inverted. This shows up clearly at point *a*.

Note that the fourth band shows the least slope or curvature; this must have been the lowest band originally. The middle band shows the most slope or curvature; this must have been the highest originally. The others can be similarly located, combining the indications from all the indicated points. Any one point is sometimes misleading due to the proximity of a harmonic to the filter boundary, as in the top band at *a*.

At points *d* and *e* there is a double inflection. This can be misleading, unless the slopes are estimated for simultaneous instants. The vertical line was drawn as a guide.

The code is 4, 2′, 1, 5′, 3′, the primes denoting inversion.

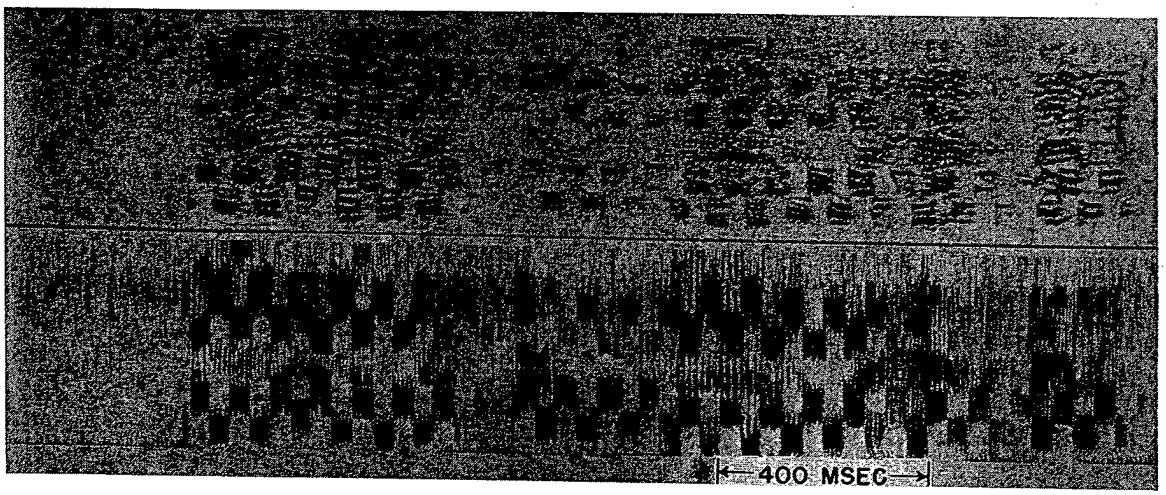



FIGURE 53. Rapidly switched split-band scramble, example 1.

These spectrograms show both horizontal and vertical boundaries. However, the level of the elements as a whole shows a rather smooth flow, as of words and spaces. Note the clear space ahead of the first word. These indications suggest that the elements have not been shuffled in time.

The presence of band shifts, however, is quite obvious. Harmonics can be seen sloping in both directions within the elements, particularly in the first word group.

The checkerboard effect in the lower spectrogram suggests that only two codes were used alternately. This is corroborated by the fact that the middle band shows no vertical discontinuities, indicating that it was never switched.

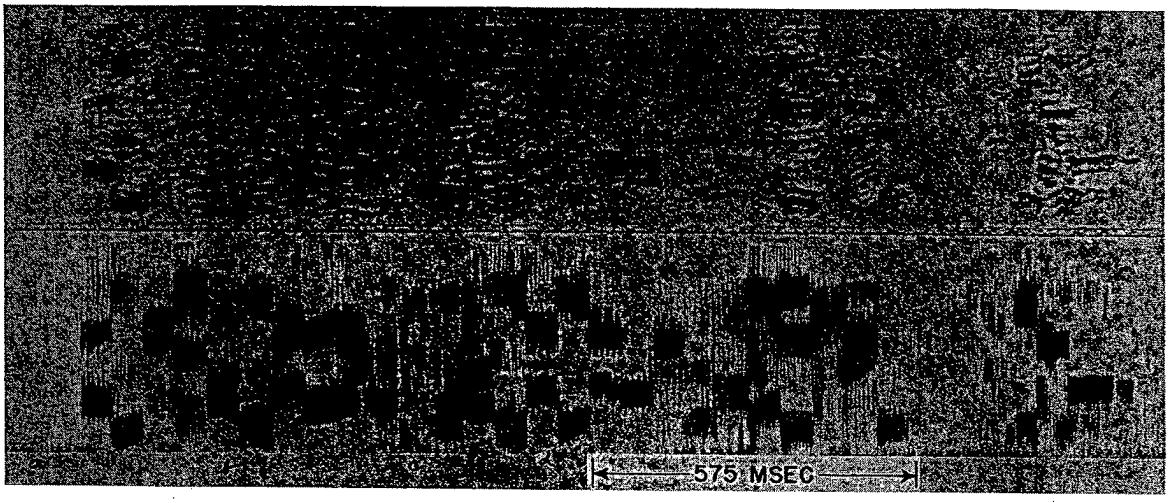



FIGURE 54. Rapidly switched split-band scramble, example 2.

Here there are both horizontal and vertical boundaries. There is no evidence, however, that the elements have been time shifted. There are unbroken clear spaces as at *a*, the long word groups such as *b* show no abrupt changes in level or in pitch, and elements having different characteristic appearance, such as those at *c* and *d*, are not intermingled.

There is abundant evidence of band shifts: harmonics sloping in opposite directions, indications of inversion, and abrupt changes in the resonance areas. Close scrutiny of long word groups such as *b* shows that several codes are being used, although it would take several samples to establish just how many.

This sample illustrates that if the codes are rapidly shifted, any one element seldom contains enough clear information to determine which code applies to it. However, if accumulated information about the system can be brought to bear, two clear bands may sometimes be sufficient to identify the code.

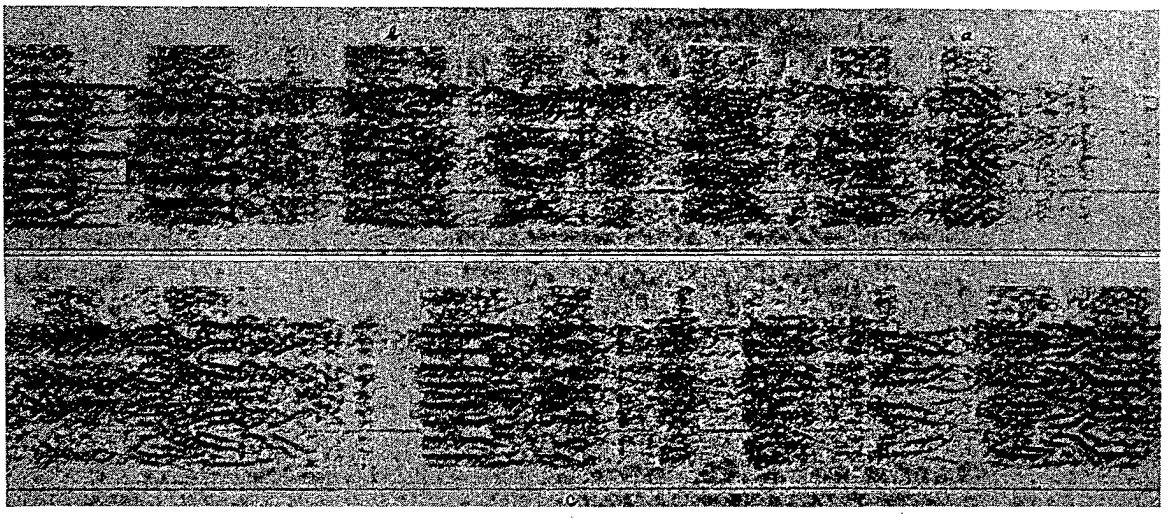



FIGURE 55. Time division multiplex.

At first glance these look like split-band scrambles. The horizontal boundaries are quite evident. The bands are 600 cycles wide, beginning at 400 cycles. It will be noted, however, that all four bands look alike, except that alternate ones are inverted. Otherwise the slopes and curvatures are alike in all bands. An outstanding example is at point *a*. There is no gradation in slope.

The components are not uniformly spaced within a band, and they frequently go in both directions within a band, as at *b* and *c*. These are the characteristics of TDM scrambling. In the particular system illustrated, the frequency range was divided into four bands, and all were modulated down to the lowest frequency. The switching rate was 600 per second, but the entire band was then modulated up 400 cycles, to avoid having the lowest sideband extend to frequencies too low for transmission channels to handle.

It is characteristic of TDM to produce upper and lower sidebands around the switching frequency and around its odd multiples. The sidebands differ only in the phases of their components.

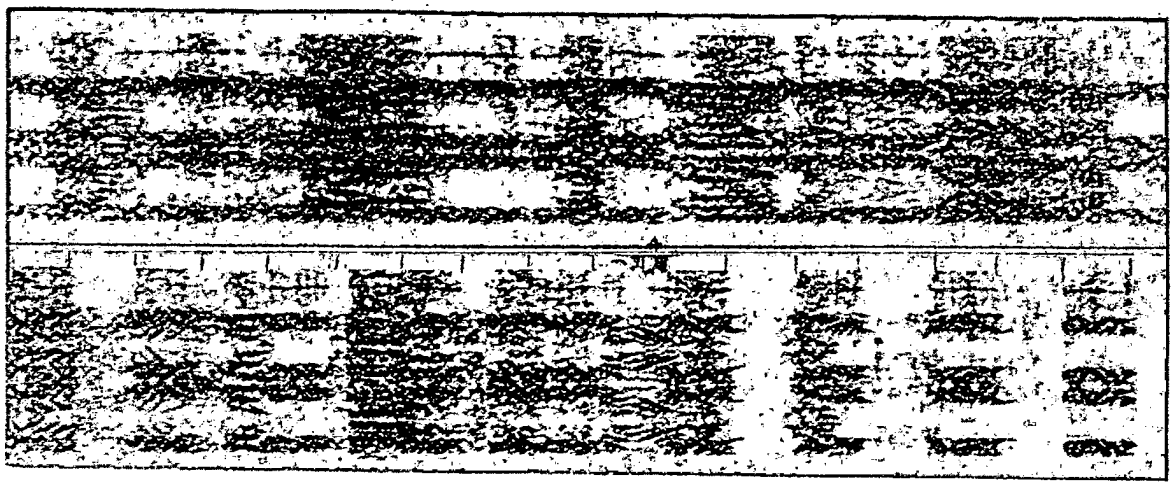


FIGURE 56. Time division multiplex with noise channel.

This is the same TDM system as in Figure 55, but a band of noise has been added to increase the privacy. One half of the highest of the four frequency bands into which the speech channel was divided has been filled with thermal noise. In the upper spectrogram of the figure, this thermal noise was steady; in the lower spectrogram, the noise was turned on and off about four times per second.

Note that although the noise was introduced into only one subband, it appears in each of the four sidebands in the above patterns. This shows that in TDM, each sideband contains components from each subband.

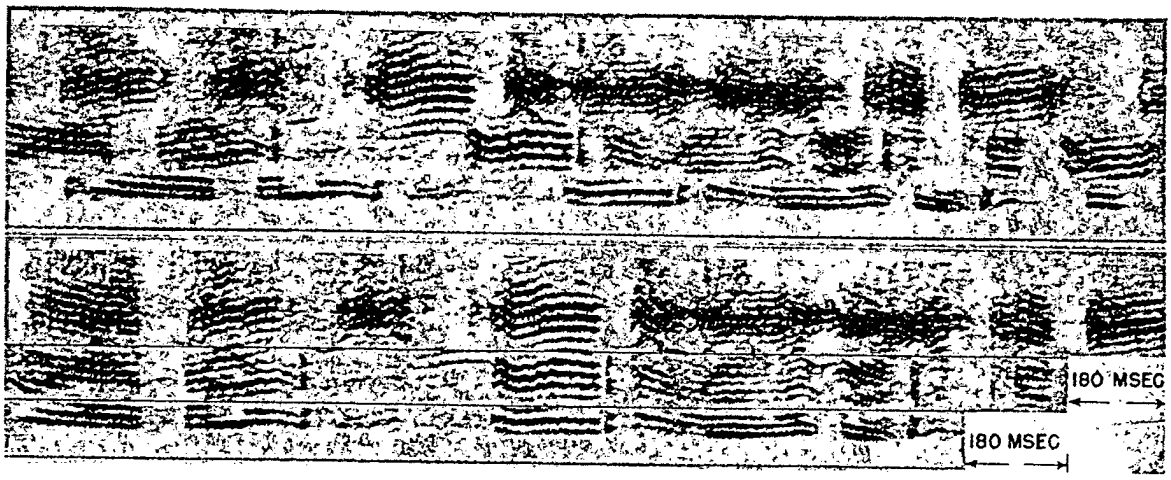



FIGURE 57. Subbands variously delayed.

Here there are horizontal boundaries, but the filters apparently do not cut off very sharply because the bands appear to overlap occasionally.

Note the staircase effect in the upper spectrogram, each syllable in the uppermost band appearing somewhat later in the middle band, and still later in the lowest band. This condition has been rectified in the lower spectrogram by cutting the frequency bands apart and shifting them relative to each other, thereby restoring the normal appearance of words and spaces.

There has been no shifting or inversion of the subbands. Note that the filter crossovers have been made very deep, as evidenced by the gaps between bands, and the lowest band has been severely curtailed in width, probably in an effort to reduce the amount of intelligence which may be gained by listening to any one band.

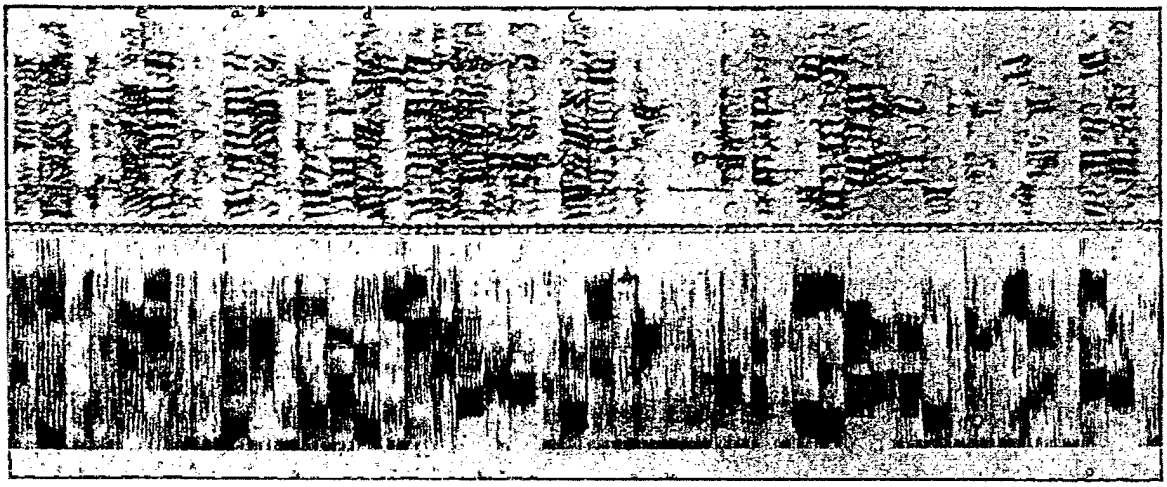


FIGURE 58. Combination of TDS and rapidly switched split-band scramble.

In this sample the evidences of band shifting are clear enough. That several different codes are used is suggested by the irregular distribution of the resonant areas over the frequency range. It is more conclusive, however, to examine the slopes of the harmonics in the upper spectrogram. At *a*, for instance, the lowest band shows more slope than either the second or fourth; at *c*, the opposite is true. At *a*, the harmonics in the second and third band slope in the same direction; at *b*, in opposite directions. To tell how many codes are used would require additional samples.

Evidences of time shifting are also clear. Elements *a* and *b*, for instance, are both strong, but are surrounded by gaps. At *d*, an element with energy distributed over the whole frequency range is surrounded by elements with entirely different distribution. There is also a marked difference in pitch between *d* and the surrounding elements. An even more marked change occurs at *e*.

This scramble, therefore, is the result of both band shifting and time shifting. It differs from a complete two-dimensional scramble in only one respect, which is described in a separate illustration.

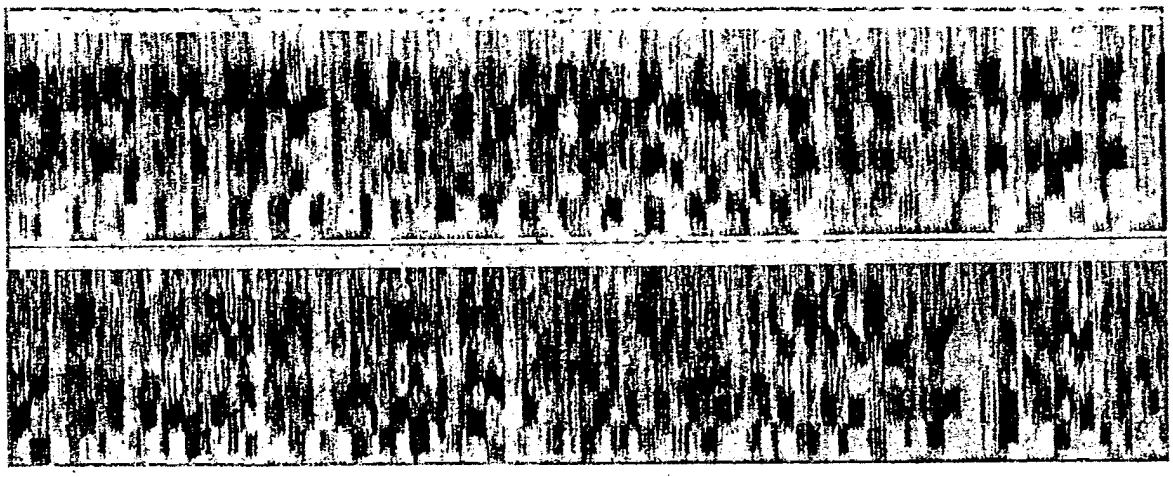


FIGURE 59. Nonsynchronous combinations of TDS and split-band scramble.

These are two combinations of TDS and rapidly switched split-band scrambles. They differ from the previous illustration in that the two switching systems are independent. The split-band code is changed at intervals of about 40 msec, whereas the length of the TDS elements is about 34 msec.

Each of these switching systems produces its own set of vertical boundaries. The distance between successive boundaries in the scramble, therefore, varies irregularly from a value corresponding to 34 msec down to zero.

In the upper spectrogram, the speech was first subjected to TDS, and then to the split-band scramble; in the lower spectrogram, the two scrambles were applied in the reverse order.

Only two split-band codes were used, alternately. Since the second scramble tends to hide the first, the upper spectrogram shows the characteristic checkerboard effect noted in a previous illustration. In the lower spectrogram, the checkerboard effect is broken up by the TDS.

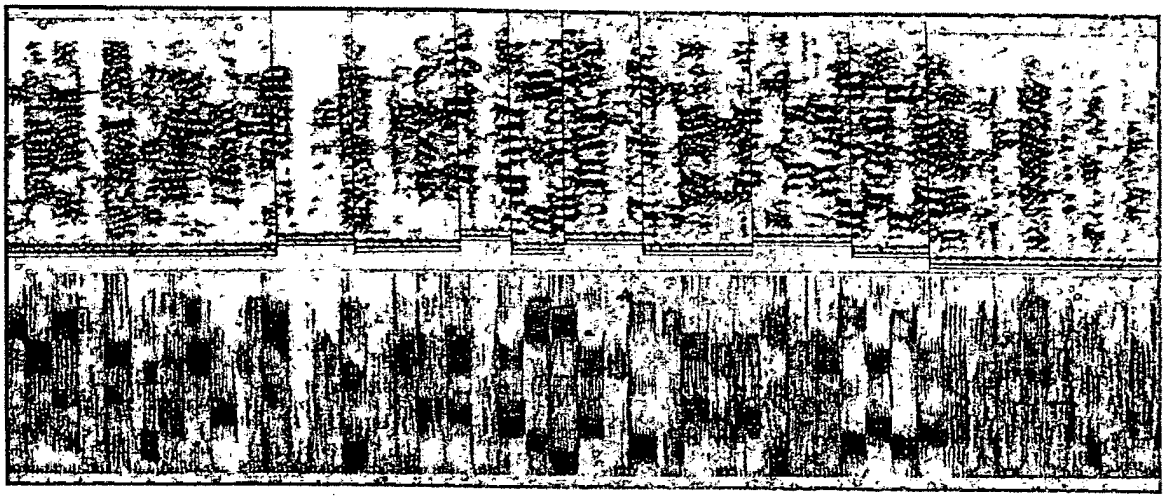


FIGURE 60. Test for two-dimensional scramble.

Spectrograms which serve to illustrate how a two-dimensional scramble might be recognized. The scramble contains both time shifts (TDS) and band shifts (rapidly switched split band). Note, however, that in either of these scrambling systems, and in the combination of both, elements which are simultaneous in the scramble (that is, subbands within any vertical section) were also simultaneous in the original speech.

In this example, therefore, a decided tendency may be seen for the character of a vertical section to remain constant over the frequency range. That is, low level elements are low all over the frequency range; high level elements tend to be high all over.

Furthermore, subbands from voiced sounds do not occur in the same vertical sections with subbands from unvoiced sounds. Voiced sound may be recognized by the presence of harmonics in the 45-cycle spectrograms, and regular vertical striations in the 300-cycle spectrograms.

The most conclusive test for a two-dimensional scramble, however, is based on the fact that there will be differences in pitch within a vertical section. This can easily be tested as illustrated above. The spectrogram is cut down the middle of a vertical section, and the pieces shifted by one harmonic in either direction. If there is no change in pitch, the harmonics will still match all over, as above. If there is a change in pitch, the shift which is correct for one subband will be wrong for another. Two-dimensional scrambles, therefore, will not pass the above test.

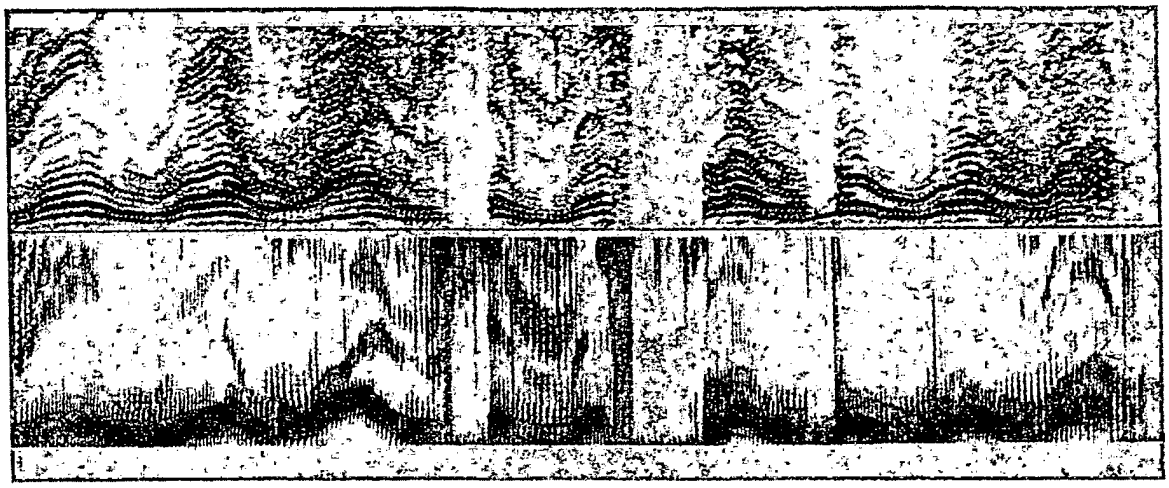


FIGURE 61. Speed wobble

The curvatures of the harmonics in the upper spectrogram look like voice inflections, except that they are abnormally frequent and rapid. The resonance areas, as shown best in the lower, also show a marked degree of curvature. Also, marked correlation may be noted between the resonance areas and the pitch, that is, they reach their high and low points simultaneously. In normal speech, the frequency and trend of the resonance areas are independent of the pitch trend. Wobbling the speed of a phonograph record or magnetic tape, however, multiplies the frequency of resonances as well as multiplying the pitch. These spectrograms were produced in this manner.

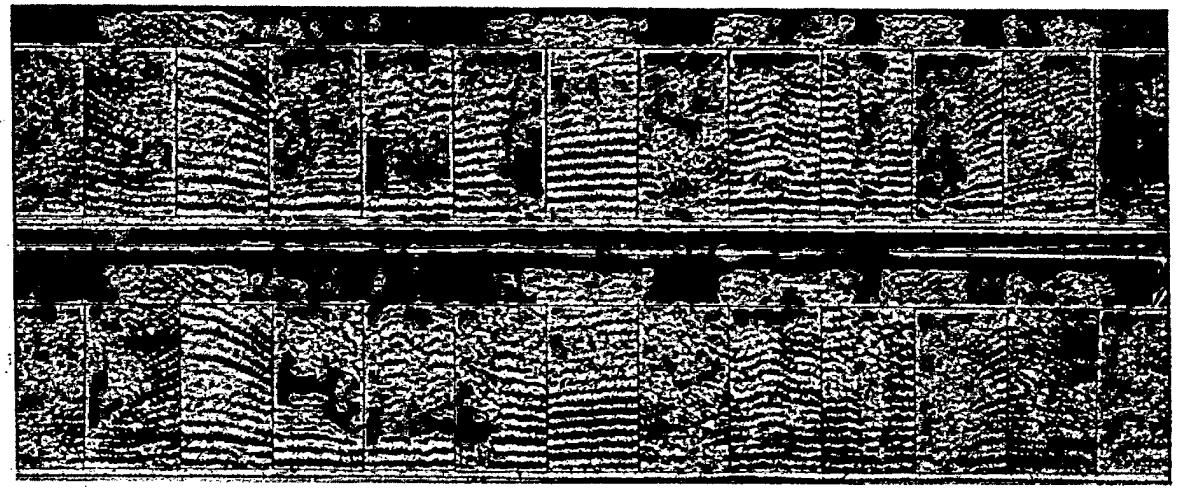


FIGURE 62. Backwards.

The above spectrograms were produced artificially by cutting up and rearranging spectrograms of normal speech.

The upper spectrogram shows the speech transmitted in sections about 160 msec long, each section transmitted backwards. If the sections are as long as this, the condition can be recognized by familiarity with the normal speech formations, that is, by the way words normally start and end, and by the trend of the resonant areas. The slopes and curvatures of the harmonics, however, look perfectly normal.

If the elements are cut apart and matched, it will be found that the right-hand edge of each element matches the left-hand edge of the preceding element. This can be seen by inspection of the above example. The order of the pieces will be completely reversed after matching. If all the pieces are inverted, however, they will be found to match in their present order.

The lower spectrogram shows the same material, but in this case alternate elements are transmitted forwards and backwards. It will be found that none of the elements can be matched together at all. To match, alternate elements must be taken from a mechanically inverted spectrogram, as described in another illustration.

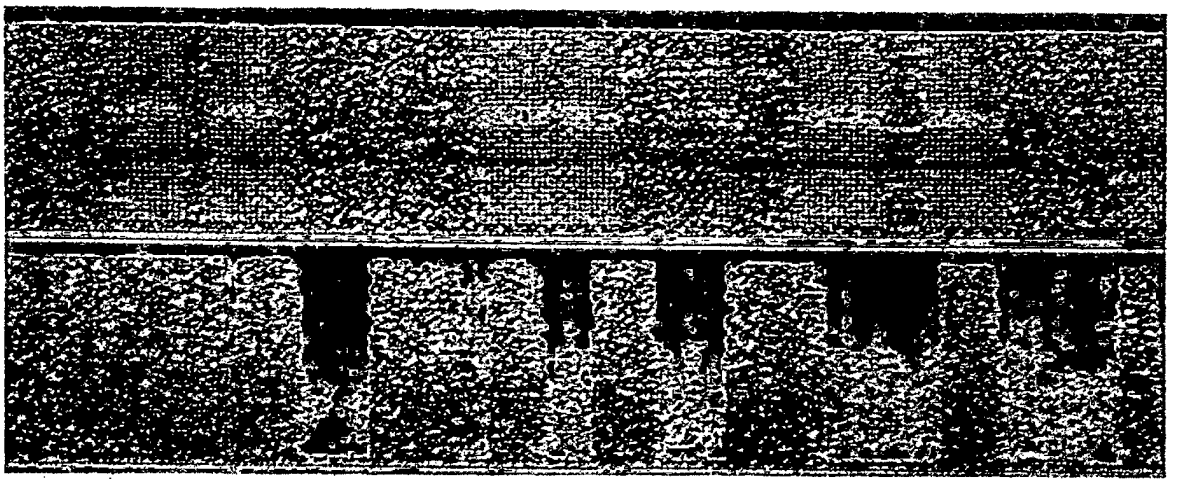


FIGURE 63. Multiplication.

The upper spectrogram shows a continuous noise, with several words or syllables showing through. Counting the harmonics shows that the fundamental of the noise is about 100 cycles.

Examination of the signal with an oscilloscope shows that the noise consists of short pulses about 10 msec apart. These can be removed by a blanking circuit.

The lower spectrogram shows a sample (not the same as the one above) without the pulses. The outstanding characteristic, as in the sample above, is an almost complete lack of the harmonic structure of normal speech. Also, the energy is distributed more or less evenly over the frequency range for each word or syllable. There are no characteristic resonance areas.

There are no regular boundaries, either vertical or horizontal. The sequence of words and spaces looks normal in the spectrogram, and has the normal cadence of speech to the ear.

These characteristics are to be expected when the scrambling system operates on the wave form directly. In this particular system, the speech wave was multiplied by a coding wave. The latter was repeated 100 times per second, with a pulse between each cycle. It is obvious that a high degree of synchronism is required to remove the coding wave at the receiving end, which accounts for the high frequency of the synchronizing pulses.

It may be noted that phase reversal (at a sufficiently high and irregular rate to achieve privacy) is also essentially a multiplication process, except that the coding wave has no values other than plus and minus unity. Spectrograms of such a system would be expected to look like the above.

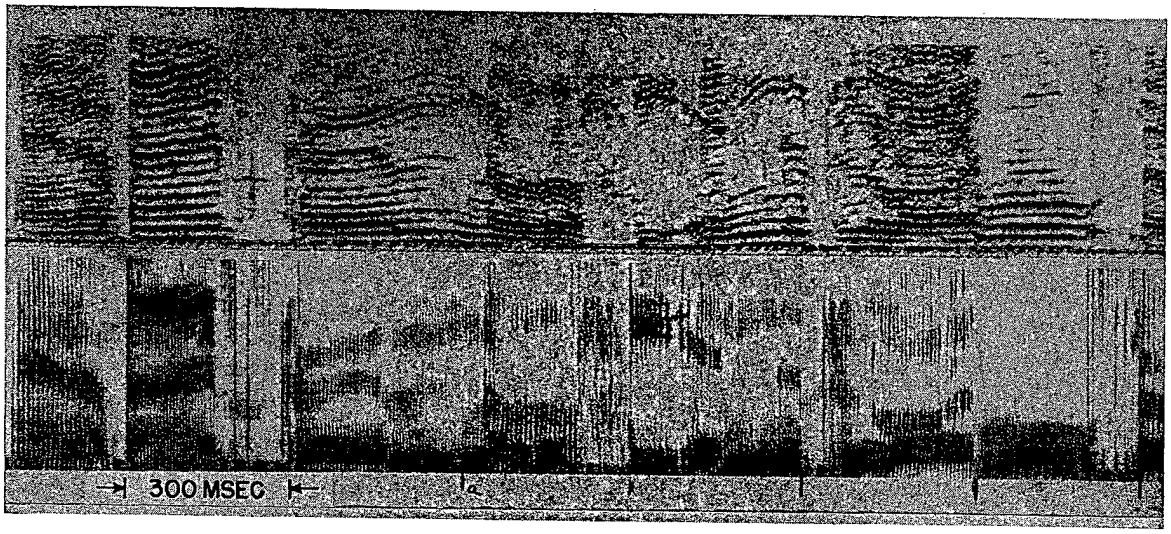



FIGURE 64. Time division channel mixing.

Here two talking circuits have been switched between two transmission channels on a time division basis, at 300-msec intervals. The vertical discontinuities can usually be seen, but point *a* is an outstanding example of apparent continuity in pitch, inflection, and resonance.

The ear can usually recognize the fact that two voices are present, at least at this switching rate. If the voices are nearly alike, or if recorded samples of the same voice are used, the nature of the scramble can be determined by cutting the pieces apart and attempting to rearrange them into continuous speech. This, of course will be found impossible in channel mixing. Another transmission channel should be found with the complementary elements.

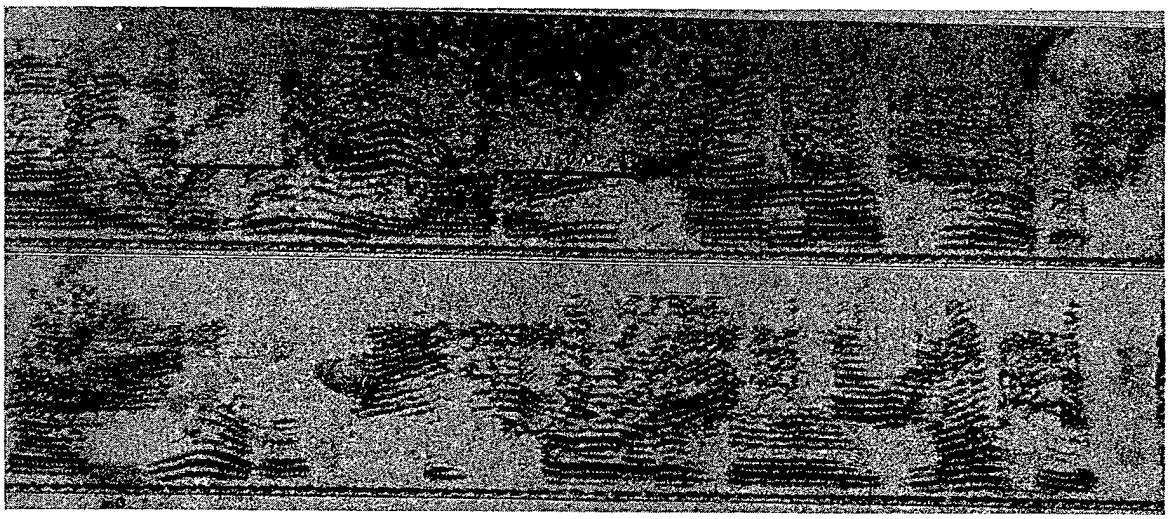


FIGURE 65. Subband channel mixing.

Here the harmonics occasionally curve in different directions, as at point *a*. A horizontal discontinuity is quite apparent at the indicated frequency, above which there are changes in pitch. These are not always readily apparent to the eye, but can be established by measurements.

In general the syllables seem to begin and end at different times in the two bands. Formations such as *c* and *d* do not occur in normal speech.

No vertical discontinuities are apparent in either band, which indicates that if any time delays are involved, they apply to the whole bands. Yet, by trial, the speech in the upper and lower bands cannot be matched by shifting the bands relative to each other.

It is apparent that two talking circuits are being switched between two transmission channels. Another channel should be found which will contain the complementary subbands. This was produced by a laboratory setup. In practice, to obtain sufficient privacy, it would probably be necessary to combine this subband channel mixing with time division channel mixing illustrated elsewhere.

Point *b*, as a matter of interest, marks an outstanding example of apparent continuity in both pitch and slope.

# Chapter 5

# DECODING PROJECTS

## 5.1 SPEECH PRIVACY PROBLEMS

STUDIES AND ANALYSES of several privacy systems of special interest to the Bureau of Ships were made under Project 13-106,[a, 34] a continuation of the work carried forward under Project C-43. In each problem the principal objectives were the determination of the security afforded by and the transmission performance of the privacy system in question.

### NATURE AND SCOPE OF THE WORK

The material submitted for study and analysis under this project comprised working models of two privacy systems, recordings of speech scrambled by three privacy systems, and paper proposals for two systems.

Security evaluations were made under favorable laboratory conditions. It was assumed that the enemy (1) was thoroughly familiar with the speech privacy system, (2) had the necessary intercept, recording, and decoding equipment, (3) had trained personnel, (4) was in a position to receive adequate signals, and (5) was completely organized so that no time would be lost in obtaining and making use of intelligence from the decoded message. The security ratings assigned to the several systems evaluated did not take into consideration any practical difficulties which might be encountered in the field or under combat conditions where the work of intercepting, diagnosing, decoding, and obtaining intelligence from scrambled messages must be carried on under stress.

The following assignments of work on this project were authorized by Division 13:

1. British Modulator Type 2C (manually switched) working models.
2. British Two-Dimensional Privacy System, recording.
3. British Modulator Type 2C (rapidly switched), recording.
4. New Zealand Switched-Band Privacy System, recording.
5. New Zealand Switched-Band Privacy System, working models.
6. Proposals of L. E. Gabrilovitch for privacy systems.

[a] Project 13-106, Contract OEMsr-1440, Western Electric Company, Inc.

### SUMMARY OF RESULTS

The results of the work done on the several assigned problems are given in detail in Reports 1 to 5, inclusive, which form an appendix to the final report of the project.[34] These reports cover the six assignments listed above with the fourth and fifth assignments, relating to the New Zealand switched-band system, being combined in one report. All of the systems considered under this project were of the short-term privacy variety. Of these, the British two-dimensional system appeared to be the most promising.

### BRIEF RÉSUMÉ OF SYSTEMS

*British Modulator Type 2C (Manually Switched), Working Models.* This system provides four fixed speech scrambling conditions, each involving either one or two simple modulating processes; the choice of any one of the four scrambling conditions or clear speech is under the control of a manual switch.

When a receiving unit, or its equivalent, is at hand, there is no difficulty whatever in discovering the proper decoding condition in a matter of seconds. The security afforded by the system is, therefore, almost nil.

The fixed-code scrambles can be demodulated satisfactorily by a single modulation process without filters, it being necessary only to use the appropriate frequency of the demodulating carrier. For this reason it is possible to obtain intelligence from radio transmissions of the scrambled speech by means of an ordinary type of radio receiver equipped with a beat-frequency oscillator. The efficacy of this method will, of course, depend upon having adequate relative stability of the radio carrier and the beat-frequency oscillator.

These units were well constructed and operated satisfactorily from the standpoint of overall speech quality.

*British Two-Dimensional Privacy System, Recording.* This system utilizes both frequency- and time-division scrambling. It employs three frequency bands and ten time elements of 0.065-sec duration in a repeated code. The time delay in one direction of transmission (exclusive of delay of the transmission path) is 0.65 sec.

The evaluation of this system was based on the study of one recording bearing a single sample of scrambled speech, together with samples of clear speech and speech which had been coded and decoded for comparison. An evaluation based on such limited data is necessarily tentative and should be supplemented by tests on working models.

The speech scrambled by this system appears to be invulnerable to direct listening and to other noncryptographic attacks. It is, however, vulnerable to cryptographic attacks and a working solution of the code can probably be obtained in a matter of 3 or 4 hours. With a model of the receiving equipment at hand, it is conceivable, although it was impossible actually to try it, that a substantial amount of intelligence could be obtained in the order of half an hour. This latter method would involve the use of spectrograms from which suggestions are obtained for setting up partial decodes on the receiving unit.

The most noteworthy weakness in the British two-dimensional system appears to be the use of a fixed repeated code. The addition of code changing means would increase the cryptographic security very greatly.

The quality of the restored (or decoded) speech presented on the recording compared favorably with the clear (or uncoded) speech on the same recording.

*British Modulator Type 2C (Rapidly Switched) Recording.* This system is the same as the Type 2C discussed above except that means are provided for rapidly switching from one scrambling condition to another and that clear speech is used as a fifth scrambling condition. The order in which the scrambling conditions are selected is predetermined according to a code which repeats after a sequence of 20 such selections, each enduring for approximately 0.065 sec.

A code-switching mechanism for use with this system was promised, but was never received. This would have made it possible to make a more positive evaluation of the system than can be made from the recording of scrambled speech. In fact, the results obtained from noncryptographic attacks on the recorded scramble are considerably at variance not only with what could logically be expected, but also with the results obtained with working models of a very similar system.[34]

Repeated listenings directly and also through a two-path superposition circuit to the recorded scramble yielded several words and phrases but very little intelligence. Similar tests on the New Zealand system (working models) yielded, on the average, 40 per cent intelligence to direct listening and 80 per cent intelligence with the two-path circuit.

Repeated listenings through an automatic analyzer-decoder circuit yielded approximately 60 per cent of the intelligence from the recorded scramble of the British Modulator Type 2C rapidly switched system. This same procedure yielded practically 100 per cent intelligence on the New Zealand system.

A cryptographic solution of the repeated-code sequence used in making the recorded scramble can be determined by inspection of two spectrograms in about 15 min.

The quality of restored speech on the recording compared favorably with the clear speech on the same recording.

*New Zealand Switched-Band Privacy System, Recording and Working Models.* Fundamentally, this system is very similar to the British Modulator Type 2C, rapidly switched, and differs in what appears to be only minor details: The inversion frequencies in the scrambling circuits are somewhat different; the duration of each of the rapidly switched scrambling conditions is 0.043 sec (rather than 0.065 sec); a sequence of 18 selections of scrambling conditions (rather than 20) comprises the coding cycle. The New Zealand system is equipped with an appliqué unit for automatically changing the code each cycle for a total of 625 cycles, or for a period of about 8 min, before repeating.

A recording of two samples of speech scrambled by this system (using repeated code) was received for analysis and most of the intelligence was obtained by noncryptographic methods. Somewhat later, the scrambling equipment for two terminal units was received and was set up for tests and demonstration as a two-way privacy system.

The security afforded by this system is very low for military purposes and is inconsistent with its size and weight.

Repeated listenings directly to the scramble yielded on the average about 40 per cent of the intelligence to experienced observers; repeated listenings to the scramble through a two-path superposition circuit yielded about 80 per cent of the intelligence. A repeated code can be determined by an aural method, using the terminal equipment, or its equivalent, in about 7 min. An automatic analyzer-decoder circuit yielded at least 50 per cent of the intelligence from either a repeated or a nonrepeated (8-min) code sequence on the first listening and practically all the intelligence with few additional listenings.

By cryptographic methods, a repeated code can be determined in about 20 min and a nonrepeated code (including the starting point of the automatic code-changing unit) can be determined in about 1 hr.

Mechanically and electrically the units operated satisfactorily; the intelligibility of the restored speech was good but the quality, though fairly good, was somewhat inferior to what might be achieved with improvements in design.

*Proposals of L. E. Gabrilovitch for Privacy Systems.* Of two proposals by Gabrilovitch, the first, described as a "Screen Secrecy Set with Narrow Audio Band," appeared to require considerable equipment to obtain only a very limited degree of security with probably poor transmission performance and a sacrifice of operating range.

The second proposal, described as a "Phase Varied Inverter-Distorter" (simplified secrecy set), although similar in basic principle to the RCA-Bedford system developed under Project C-54[14] offered, theoretically, some possibilities of obtaining a fairly compact and lightweight set having somewhat better restored speech quality than the Bedford system. There were, however, a number of questions regarding the degree of security, coding possibilities, and practicability of some of the electronic processes.

When, after study, it appeared fairly evident that the development of the second proposal would tend more and more to duplicate that of the Bedford system and would offer few, if any, advantages over the latter when completed, it was recommended that further study of this proposal be discontinued.

### General Conclusions and Remarks

In the course of the work done under this project, a number of conclusions were reached regarding the systems under consideration and their evaluation based on the use of working models as contrasted with phonograph recordings.

*Switched-Band Systems.* Of the systems considered, vulnerability to repeated listenings directly to the scramble is attributed to the inherent lack of privacy in some of the five speech-scrambling conditions. The average intelligence obtained in listening to the five fixed scrambles is 40 per cent, which is approximately the same as obtained (on the average) when the scrambling conditions were rapidly switched. The need for scrambling conditions, each having an adequate degree of privacy, is obviously indicated.

The high yield of intelligence obtained from superposition listening is attributed mainly to the fact that some of the five scrambling conditions are not mutually private and effectively decode one another (Codes A and B in the New Zealand system and Codes 1 and 3 in the British system). This effectively reduces the available number of scrambling conditions. Hence, the five scrambling conditions should be not only inherently private but also mutually private.

The vulnerability of the systems to either direct or superposition listening is independent of whether a repeated or nonrepeated code is employed.

The use of a repeated code makes the system very vulnerable to methods of cracking wherein the code is to be determined. It is necessary to

decode only one cycle when successive cycles can be used to obtain confirmation.

When the system is not vulnerable to noncryptographic attack, the use of nonrepeated coding increases privacy. If the coding is truly random, it is necessary to decode each individual cycle with no opportunity for confirmation from successive cycles.

*Two-Dimensional System.* This type of system involving both frequency and time division scrambling affords more security than can be obtained by using either method of scrambling alone. In the case of the British system considered, the privacy would have been materially increased by using a nonrepeating code, more frequency bands, and shorter and more time elements.

*Masking Systems.* Systems of this type employ a screen of noise overlaying the signal to be masked. This is accomplished in one system by modulating the masking and masked signals on a split-phase subcarrier. The discrimination between these two signals at the receiver requires absolute synchronization and proper phasing of the demodulating carrier. Since this is difficult to achieve in practice, because of the distortions appearing in the transmission channel, the restored speech will be of poor quality, being distorted and noisy.

The relatively large amount of power required for the masking signal reduces the efficiency of the radio transmitter in that smaller transmitting ranges are obtained for a given amount of output power.

*Bedford Type Systems.* Systems of this type, of which the phase-varied inverter-distorter system proposed by Gabrilovitch is one, depend upon the modulation of speech by a complex coding wave to obtain privacy. Clear speech is obtained at the receiver by demodulation of the scramble with an accurately synchronized decoding wave which effectively is the reciprocal of the coding wave.

To avoid the possibility of partially cracking the scramble by demodulating it with a single frequency, it appears to be necessary that the complex coding wave have no predominant frequency components but, instead, should have a fairly uniform spectrum of at least several hundred cycles width within the limits of the speech band. The resulting band width of the scrambled speech exceeds the width of the speech band by an amount equal to the highest frequency in the coding wave. It follows, then, that either the band width of the channel conveying the scrambled speech must be wider than for normal speech bands, or the original speech band must be made narrower than normal if distortion is to be avoided.

Since an accurately synchronized decoding wave of proper phase is required for deriving clear speech at the receiver, this system is sensitive to distortions in the transmission channel. The restored speech should not, however, be as noisy as that of the masking systems. In the Bedford type systems, imperfect demodulation yields unwanted products which are proportional to the speech energy rather than to the relatively large masking energy.

Synchronization by means of a continuous modulated wave is believed to be superior to synchronization by pulses as proposed in the RCA-Bedford system. In the latter instance, the wave form of the transmitted pulse is both important to the proper operation of the system and sensitive to distortions over a large part of the band of the transmitting channel.

*Evaluation of Security of Systems from Recordings.* Phonograph recordings of speech scrambled by a privacy system provide a less desirable means for evaluating the security of a privacy system than do working models of the system. The results of analyses based on phonograph recordings can be used for determining the nature of the privacy system and the code but even though the quality of the recording is good, difficulty may be experienced in direct or superposition listening tests.

Very often it is found that recordings, which are considered moderately good for clear speech are surprisingly inadequate for storing scrambled speech for subsequent analysis and restoration. This appears to be due to (1) harmonic distortion, which, when not too great, passes unnoticed in clear speech, and also to (2) irregular speed variations (in either the recording or reproducing systems) which prevent precise synchronization necessary in some privacy systems. However, the fact that a high quality recording is required in cracking a

given privacy system, is in itself, of considerable practical importance in evaluating the system.

The most effective cracking techniques often involve the use of a receiving unit, or its equivalent. When only recordings are available for analysis, it becomes necessary either to build an equivalent receiver or merely to speculate on what might be done with a working model. Neither of these alternatives is very satisfactory. It is, therefore, highly desirable whenever possible, that evaluations be made by tests on working models.

## 5.2 FIELD DECODING EQUIPMENT

The experience gained with the sound spectrograph in Projects C-32 and C-43 resulted in the recommendation that the device be redesigned for field use and included in field decoding kits at radio intercept stations. Under Project 13.3-86[b] eight of the units were built, three for the Signal Corps, three for the Navy, and two for the British under Lend-Lease requisition. Together with operating and maintenance instructions, these eight spectrographs (D-165-529) were delivered between January and May 1, 1944.

The units had the following weights and dimensions:[35]

| Unit | Weight | Dimensions (Inches) |
|---|---|---|
| Recorder | 68 lb | 17½x16½x11¾ |
| Amplifier-analyzer | 64 lb | 20¼x11¼x14¼ |
| Rectifier | 56 lb | 20¼x11¼x10¾ |

[b] Project 13.3-86, Contract OEMsr-1110, Western Electric Company, Inc.

# Chapter 6

# FACSIMILE PRIVACY SYSTEMS

## 6.1 INTRODUCTION

THE SCRAMBLING SYSTEMS heretofore described have related to the transmission of speech. Another important form of communication, however, is graphic copy such as maps, drawings, and photographs, where a facsimile of the original subject copy is to be transmitted to a remote point by wire or by radio. In wartime, of course, it is as important that privacy be attained in this form of communicated intelligence as in the transmission of the human voice.

Two projects under Division 13 were concerned with the general problem of scrambling graphic copy, Project C-73[a] being a survey of all existing and proposed systems and Project 13.3-97[b] describing a system for scrambling the copy before scanning it for transmission by radio or wire.

## 6.2 FACSIMILE PRIVACY

### 6.2.1 Statement of the Problem

At the time of this project, all concerned agreed that facsimile had attractive possibilities as communication means, but up to that time it had been handicapped by lack of privacy for military use. Considerable information on the several phases of the subject existed in various places but no attempt had been made to consolidate it. Accordingly Division 13 authorized Project C-73 which had as its object the survey of the general field of facsimile privacy and the preparation of a report on the subject.

The project was completed between December 1942 and July 1943. A final report[36] was prepared on June 7, 1943, and a much abridged report of this final report on October 15, 1943. The summary to follow is taken from the abridged report. Since it is the basis of any further work in this subject, this abridged report is summarized in some detail. The complete final report gives essential details of nonprivate systems and furnishes complete background.

The directive covering Project C-73 called for:

1. A brief summary of basic facsimile mechanisms and modes of transmission.
2. Investigation of the degree of privacy obtainable.
3. Adaptability of telephonic privacy systems then existing and those under development.
4. Evaluation of means for cryptanalysis of various graphic privacy systems the enemy may use.
5. Suggested design of the most useful type of equipment for both privacy transmission and cryptanalysis.

The contractor made contact with all known individuals and organizations in the United States who might be able to contribute suggestions which would be useful in providing facsimile privacy. A complete report on these contacts is given in the appendices of the final report. At the time of the survey, telephonic scrambling methods were under active study by Division 13 contractors and by the Military Services, but up to that time no attempt had been made to use telephonic systems for facsimile privacy.

Laboratory tests were made to determine the effectiveness of telephone systems as applied to facsimile. Throughout the investigation of all known and suggested methods of privacy for graphic copy, the attempt was made to consolidate the acquired data on means of applying the systems studies, and on the effectiveness and availability for production and other points of interest to the Services.

### 6.2.2 Privacy Defined

A coded facsimile subject may be considered to have been rendered *secret* when it is so coded

[a] Project C-73, Contract OEMsr-837, Radio Corporation of America.

[b] Project 13.3-97, Contract OEMsr-1202, Faximile, Inc.

that no means may be improvised to decode it, other than use of the applied code and equipment. This is the ideal condition, but one which was unattainable in practice.

A coded facsimile subject may be considered to have been rendered *private*, from a military point of view, when at least 72 hr are required to reproduce the essential intelligence of the original subject copy. If the subject copy is a map, the essential intelligence is obtained when locations are disclosed. If the subject copy is type, the essential intelligence is disclosed when the characters become legible, regardless of decoded subject quality.

The relative degree of privacy of a coded facsimile subject may consequently be estimated by the number of hours required to decode its essential intelligence. This time may sometimes be reduced by subdivision of decoding operations among several members of a decoding staff.

### 6.2.3 Facsimile Coding Methods

A facsimile signal is less vulnerable to unauthorized reception than ordinary voice or code signals because it is unintelligible unless one has a recorder. With a recorder available, however, which can be readily adjusted over a wide range of drum speeds, it would be a matter of less than a minute to establish the correct operating conditions to receive a picture. It must be assumed that the enemy has such apparatus and that, therefore, additional privacy means are essential for military transmission.

Unlike voice transmission, the sending of intelligence by facsimile depends on two parameters. The first is the continuous envelope of signals representing the shading of successive picture elements. The second is the information as to where each successive picture element should be printed on the recording sheet in order that a picture may be formed. This is normally supplied by moving the scanning spot through a fixed and simple scanning pattern at a known rate of speed. Obviously, privacy can be secured

1. By scrambling the signal transmission,
2. By confusing the scanning pattern,
3. By both scrambling the signal transmission and confusing the scanning pattern.

The facsimile picture signal is ordinarily a modulation on a subcarrier and can be transmitted through the same apparatus and circuits as are used for voice signals. For low-speed facsimile the channel width required is also of the same order. Thus, already developed methods of voice scrambling can be considered for facsimile privacy. There are three of these, the first three in the following tabulation.

#### Six Basic Methods

The assigned designations below are used throughout the rest of the report.

1. [A] Transposition of frequency bands.
   The spectrum of signal frequencies is divided into five bands and these are manipulated to secure privacy.
2. [B] Frequency multiplication.
   All signal frequencies are multiplied by a complex and changeable coding wave to produce a new pattern of frequencies within the transmitted spectrum.[14] (See Chapter 3.)
3. [TDS] Time delay system.
   The signal envelope is divided into intervals of time, which intervals are variously delayed and then transmitted in a new order.

When these three speech scrambling systems are applied to facsimile, the first two scramble the signal; the last one, however, is equivalent to a confusion of the scanning pattern and it can be most clearly thought of in that way. It is just as if the scanning spot traversed one part of a line of the subject, then jumped to another part, and so covered the whole area in an irregular sequence of partial scanning lines.

To these already developed and self-contained coding means there may be added the following:

4. [PR] Polarity reversal.
   Parts of the scanning line are reversed in polarity, from black to white and vice versa, according to a coding sequence.

5. [VS] Variable speed.
   The scanning pattern is modified by changing the drum speed by varying amounts according to a coding sequence.
6. [PT] Pretransmission.
   The subject copy is itself scrambled by optical or other means before being placed on the scanner.[36] (See Section 6.3.)

Methods 4 and 5 involve special modifications of the normal facsimile equipment. Method 4 can be thought of either as a distortion of the signal envelope or a confusion of the scanning pattern; Method 5 is obviously the latter. Method 6 has grown out of the activity of this project but is, of course, not limited to facsimile. It would be equally applicable to messages delivered by courier.

It should be emphasized that the very orderliness of the normal facsimile process makes difficult the successful application of privacy methods to picture transmission. Any cyclic switching operation will reveal its true time sequence in the facsimile reproduction. Line sections must be exactly fitted to avoid gaps or overlap. Even the white picture background may reveal coding changes due to slight exposure variations. Long, straight lines normal to the direction of scanning are particularly revealing since they serve as time references, and disclose periodicities. In fact, the reproduced facsimile copy is a permanent record of all the optical and electrical operations which have been performed on the subject copy. Unlike the scrambled radio-telephone sound wave, it is permanently captured to lure to the fullest extent the ingenuity of the decipherer.

### Nomenclature for Various Methods

To facilitate the designation of the various secrecy methods, a nomenclature was adopted in the final and abridged project reports in which the basic systems are indicated by letter combinations. In addition to the letters, a numeral is appended to differentiate between specific types of a basic system. If two basic systems are operated in combination, the letter group of each system will be used. These designations are as follows.

*Transposition of Frequency Bands* [*A*]. The method of subdividing the picture signal into discrete frequency bands and interchanging these bands in the frequency spectrum in accordance with a coding signal is designated by the letter A. A modification of this method includes the process of frequency inversion.

A-1 and A-2. These designations are left open for experimental development.

A-3. This is the standard commercial system of the Western Electric Company.

*Frequency Multiplication* [*B*]. The method of transmission whereby a coding signal is multiplied into an intelligence signal is designated by the letter B. Modifications of this basic system are essentially modifications of either the intelligence signal or the coding signal.

B-1. Straight multiplication without alteration of the intelligence signal or the coding signal.

B-2. An audio tone of fixed amplitude and of a frequency outside of the picture signal band has been added to the intelligence signal.

B-3. An audio tone of fixed amplitude and of variable frequency outside of the picture signal band has been added to the intelligence signal.

B-4. The normal subcarrier frequency modulation [SCFM] modulated with a 500-cycle tone.

B-5. The normal SCFM picture signal is limited; i.e., the sine wave of varying frequency is converted to a square wave of varying frequency before multiplication.

B-6. A very low frequency (less than 1 cycle per second) has been added to the picture before conversion to SCFM and subsequent multiplication. This results in a slow shifting of the picture signal band in the frequency spectrum.

B-7. A method wherein the coding signal is changed periodically. The equipment for this system has been named "Myopia Mark I."

*Time Delay System* [*TDS*]. Essentially, this method produces a continuous transmission of coded signals by breaking down the normal signal sequence into discrete time-signal intervals and rearranging these intervals in a different chronological order. Modifications of this system are made on the basis of the total

number of signal intervals that can be switched.

TDS-1. This is the Model B magnetic-tape system as developed by the Bell Telephone Laboratories [BTL].

TDS-2. This is the D-Specification magnetic-tape system as developed by BTL.

TDS-3. This is the C-50 magnetic-tape system as developed by BTL under Project C-50.[10]

TDS-4. This is a simple two-head magnetic-tape system as used in the preliminary tests on this project. The time delay between the two heads was approximately 1/20 sec.

*Polarity Reversals* [*PR*]. This method is designated by the letters PR. Basically, it is a system which subdivides a continuously varying picture signal into time intervals and determines the polarity of the transmitted signal throughout these intervals. The process can be visualized as a reversing switch controlled by an auxiliary or coding signal which interchanges the black and white portions of the picture. The degree of confusion will then be directly proportional to the rate of switching. Therefore, the applications of the basic method are subdivided into the following forms.

PR-1. Polarity reversals in which the time of transmission of one polarity is greater than the time of transmission of a scanning line. The coded picture will then be composed of groups of scanning lines of alternate polarity and the number of scanning lines in any group will vary with the duration of the coding signal.

PR-2. Polarity reversals in which the time of transmission of one polarity is less than the time of transmission of a scanning line. With this arrangement, every scanning line of the coded picture will resemble a chain whose alternate links have reversed polarity.

PR-3. This method is similar to PR-2 except that the duration of the switching polarity is decreased until it approximates that of a picture element.

*Variable Speed* [*VS*] *and* [*CVS*]. In a variable-speed transmission system, the linear speed of scanning is varied in accordance with a coding signal. In practice, this variation may be in fixed steps [VS], or continuously variable [CVS]. It represents a modulation of the scanning rate, and may vary from a small percentage of the scanning rate to 15 per cent or more.

Speed deviation classifications have been designated as indicated below:

VS-1. Speed change code of $\pm 1/2$ per cent.

VS-2. Speed change code of $\pm 1$ per cent.

VS-3. Speed change code greater than $\pm 1$ per cent.

VS-4. Two dimensional VS scanning for PT method.

CVS-1. Continuously variable speed change code.

*Pretransmission* [*PT*]. Methods wherein the subject copy is itself scrambled by optical or other means before being placed on the scanner.

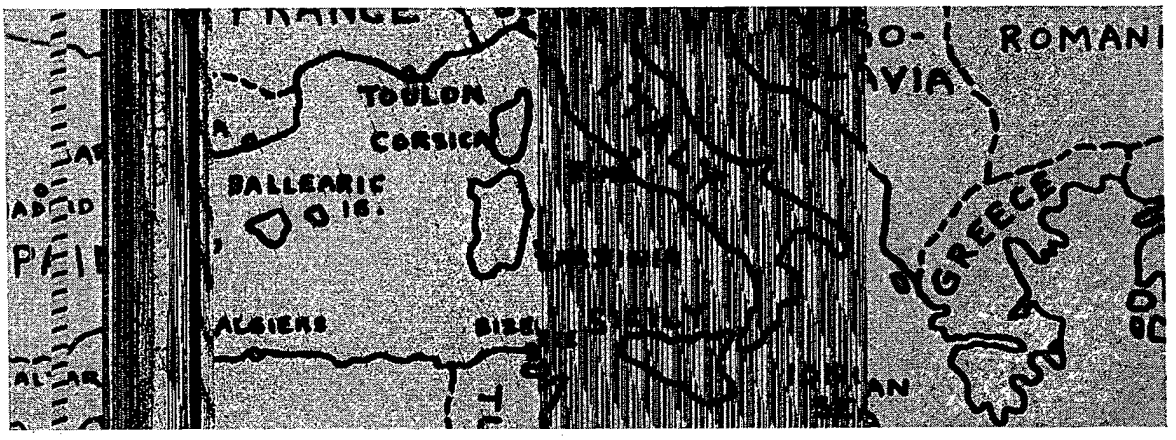



FIGURE 1. Map uncoded (right), coded by frequency transposition (middle), and decoded (left).

SECRET

## Typical Samples of Coding and Decoding by Various Single Privacy Methods

*Transposition of Frequency Bands* [*A*]. Figure 1 is a typical example of coding and decoding with the existing Western Electric speech privacy equipment A-3. The right portion of the recording is the uncoded subject copy; the middle section, coding by five test frequencies; and the left section, the decoded copy.

*Frequency Multiplication* [*B*]. Figure 2 is a typical example of coding and decoding with the Myopia Mark I equipment. The right section shows the coded picture using 3-sec normal code shift; the center section, the decoded copy; and the left section, the normal uncoded subject copy.

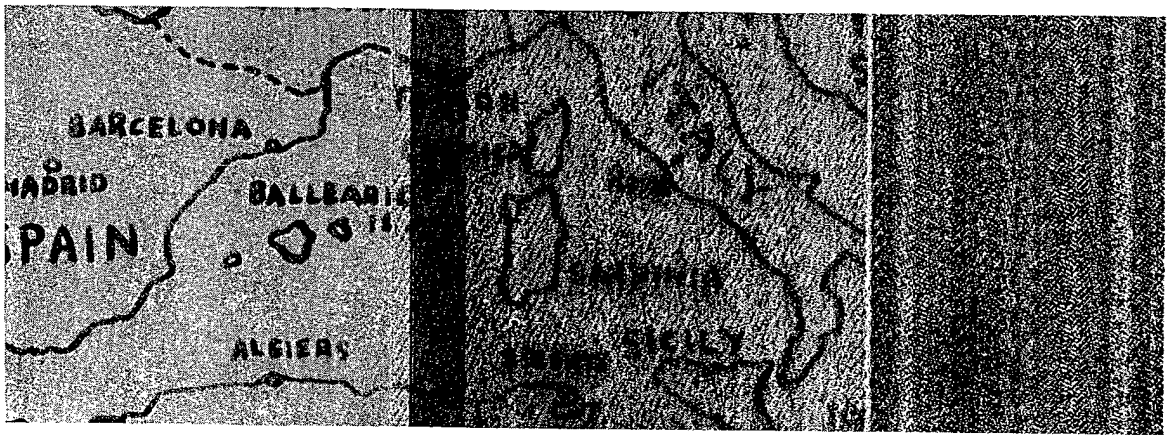



FIGURE 2. Copy coded by frequency multiplication (right) and decoded (middle).

Mathematical analysis indicates that method B should be subject to decoding by means of a filter placed at the frequency corresponding to either white or black, by virtue of the differentiating action of the photocell at the boundary. Figure 3 shows the effect of passing the coded signal through a 100-cycle narrow-band filter having a 1,445-cycle mid-frequency, which cor-

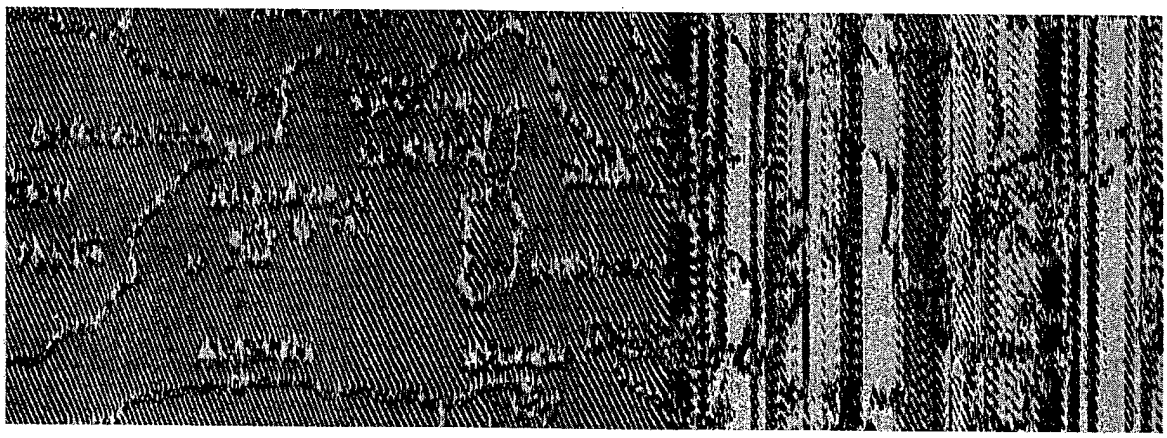


FIGURE 3. Effect of passing coded signal of Figure 2 through narrow-band filter. Left half employed only one coding wave; right half used 3-sec code shifts.

The coded section is seen to introduce a background, without scrambling of the essential intelligence. The system has no privacy when applied to facsimile transmission.

responds to white in the recording. The left half of the recording utilized only one coding wave, the right half employed 3-sec code shifts. The essential intelligence of the subject copy is seen to be revealed by filter decoding.

Figure 5 is the result of coding by polarity reversals at the rate of approximately 50 per scanning line. The left portion of the recording is the result of applying a telegraphic signal repeating every 80 bands, as an additional

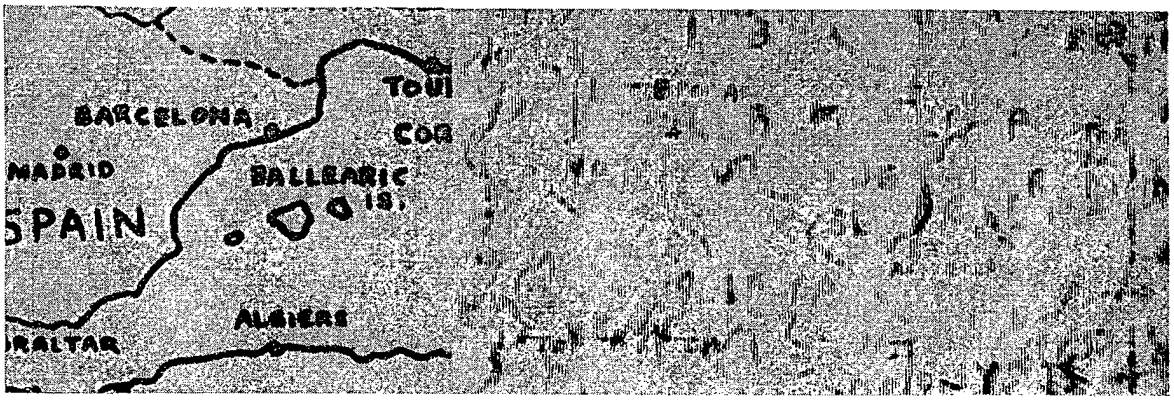



FIGURE 4. Map scrambled by TDS system. Left portion is decoded version of map.

*Time Delay System* [*TDS*]. Figure 4 is a typical example of coding and decoding by the D-Specification TDS system. The right portion of the picture shows a complete scramble with little evidence of switching periodicities. The left portion of the picture is the reconstructed subject copy resulting from the decoding operation. D-Specification TDS is an immediately available system, having a high degree of viewing privacy, and a considerable degree of decoding privacy.

*Polarity Reversals* [*PR*]. Figures 5 and 6 are typical samples utilizing the PR method. coding source. Boundary conditions are seen to convey a considerable degree of intelligence in both sections of the coded picture.

Figure 6 is the decoded version of the above coded picture. It shows a reproduction of the subject copy, with good quality.

The susceptibility of the PR method to de-

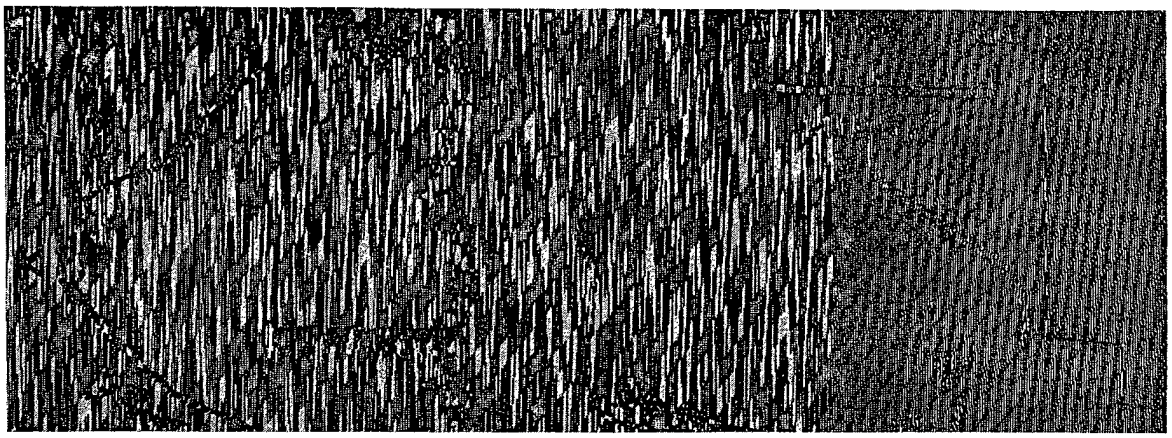


FIGURE 5. Appearance of copy scrambled by polarity reversal.

coding by switching transients passed through a narrow-band filter is shown in Figure 7. In this recording the switch reverses polarity at the rate of approximately 50 times per scanning line. The left portion of the picture is normal uncoded subject copy, the middle sec-

tion coded, and the right section decoded by passing the 1.5- to 2-kc f-m signal through a 100-cycle narrow-band filter having a mid-frequency of 1,785 cycles. The recording is seen to be completely decoded by the filter, as far as essential intelligence is concerned.

drum at normal drum speed will be noted in the coded section of the recording.

The CVS method, at the same maximum frequency deviation of ±5 per cent, is illustrated by Figure 9 made by Times Telephoto Equipment, Inc., using continuously variable drum-

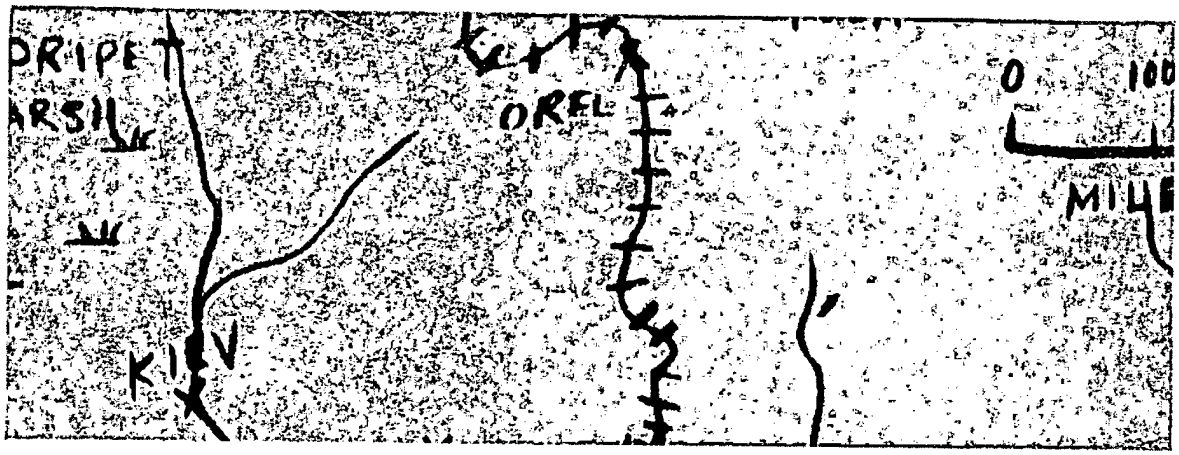



FIGURE 6. Decoded version of Figure 5.

*Variable Speed [VS] and [CVS].* A typical recording by the VS method is illustrated by Figure 8. A speed deviation having a maximum of ±5 per cent was applied for a fixed number

speed shift, but with a random drum-speed swing. The lower section of the picture is normal uncoded, the middle section coded, and the upper section synchronously decoded. The

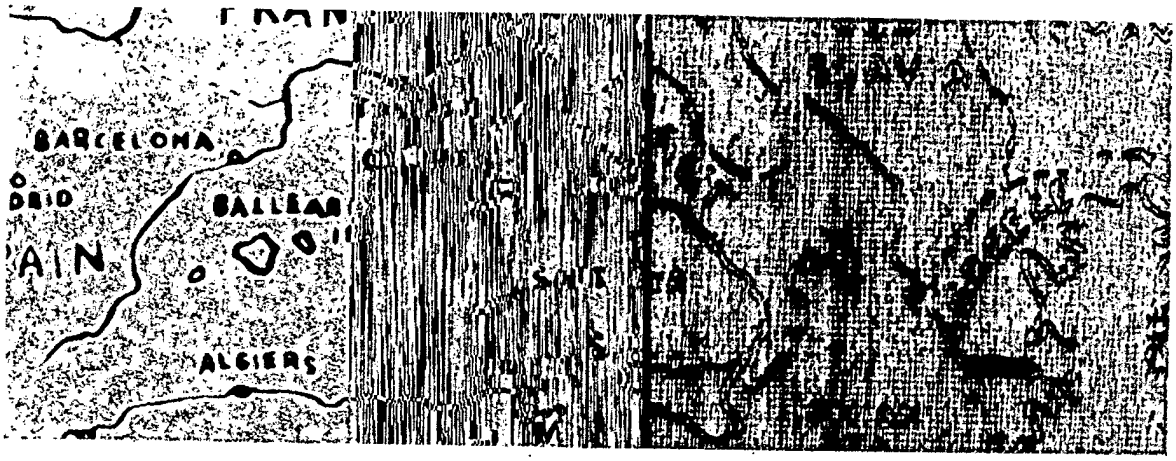



FIGURE 7. Example showing susceptibility of PR system to decoding by passing coded signals through narrow-band filter. Left portion, uncoded copy; middle portion, coded by PR; right portion, copy decoded by use of filter.

of drum revolutions varying from 10 to 20 per frequency step. The lower section of the recording is normal uncoded, the middle section coded and the upper section decoded. A decoded strip corresponding to ten revolutions of the

CVS method shows the highest degree of privacy of the single methods. No direct *electrical* method has as yet been devised to break the CVS code.

*Pretransmission [PT].* The pretransmission

method PT has not been developed experimentally to the stage in which coded and decoded subject copy is available by facsimile transmission. The possibility of the method for coding purposes is shown in Eastman Kodak Company samples, Figure 10, in which a double shredding process was used. At the lower left of Figure 11 is shown a coding by the single shredding process, and at the lower right a second shredding at right angles to the first.

The method is limited as to its basic privacy by the problem of registration and skew which will determine the practical element size. The method gives promise of being particularly valuable as a combination method with TDS or CVS.

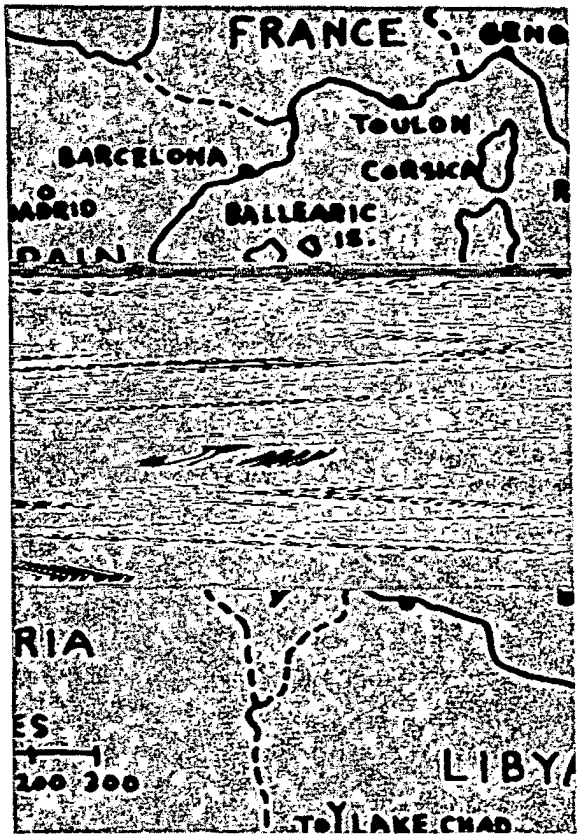



FIGURE 8. Recording by variable speed [VS] system. Lower portion, normal uncoded; upper portion, decoded material.

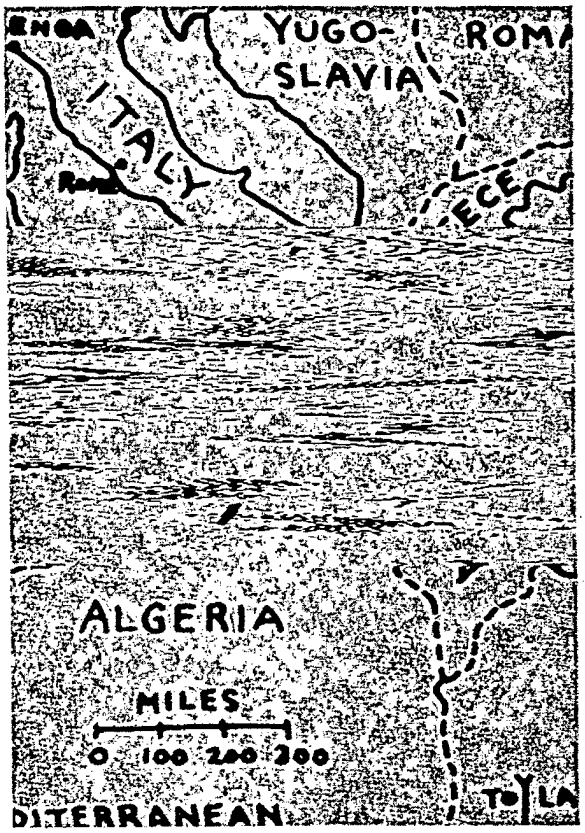



FIGURE 9. Scrambling by continuously varying drum speed.

### CODING AND DECODING BY TANDEM COMBINATIONS OF PRIVACY METHODS

*Polarity Reversal [PR] and Time Delay [TDS] in Combination.* The PR and TDS combination is illustrated by Figure 12. Mixing of the two methods produces a high degree of privacy for the combination. Difficulty of synchronization and phasing at the scanner and recorder, unfortunately, renders the combination less attractive for practical circuit applications.

*Transposition of Frequency Bands [A] and Time Delay [TDS] in Combination.* The A and TDS combination is illustrated by Figure 13, made by using the standard A-3 Western Electric speech privacy system with the BTL Model B TDS system. The right section shows normal recording without A or TDS; the middle section is the coded picture utilizing the coders of A and TDS in combination; and the left section is the decoded copy resulting from passing the coded signal through the tandem decoders. Reference to the coded middle section shows that a single system having no privacy by itself may be raised, by combination with another

single system, far above that of either component system used singly.

*Variable Speed [VS] and Time Delay [TDS] in Combination.* The TDS and VS combination is illustrated by Figure 14. The single methods used in this combination are D-Specification TDS and a step-by-step variable speed VS at the rate of $\pm 1/2$ per cent. A remarkable increase in visual scrambling is attained compared to using the single method alone.

*Frequency Multiplication [B] in Combination with Variable Speed [VS].* Figure 15 is the result obtained with the B and VS combination. The Myopia Mark I coder and decoder was used in applying the B coding. SCFM recording with a subcarrier frequency of 1,380 to 1,750 cycles was applied. The coder was operated on a 3-sec continuous-code shift with constant amplitude into the unit. VS was applied at the rate of $\pm 1/2$ per cent speed deviation.

The right portion of this illustration is the coded subject; the middle section, decoded by passing the coded signal through the decoder and varying the drum speeds in synchronism; and the left section, the uncoded subject copy.

The B and VS combination is less attractive from an application viewpoint due to the relative ease with which B may be decoded by a narrow-band filter intercepter.

## Practical Applications of Privacy Methods

Transposition of frequency bands [A] is represented by the Western Electric Type 3-A speech privacy equipment. It is fixed station equipment of large bulk and weight.

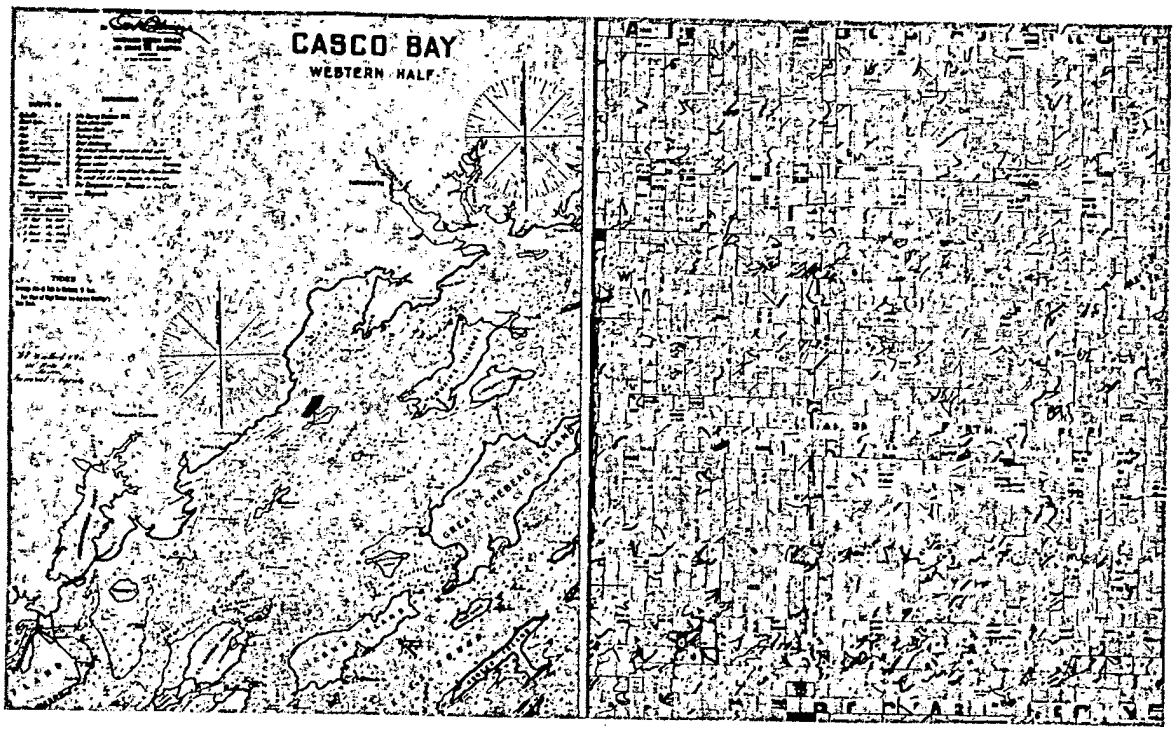



FIGURE 10. Example of pretransmission scrambling.

The method depends upon fixed interchange of frequency bands. There is no automatic synchronization or phasing problem. The method has been shown to give no privacy when applied to facsimile transmission.

Frequency multiplication [B] is represented by Model RCAL-1[14] weighing 32 lb and having a volume of approximately 3/4 cu ft. The code is set up on numbered dials, with provision for continuous change by means of a clock mechanism.

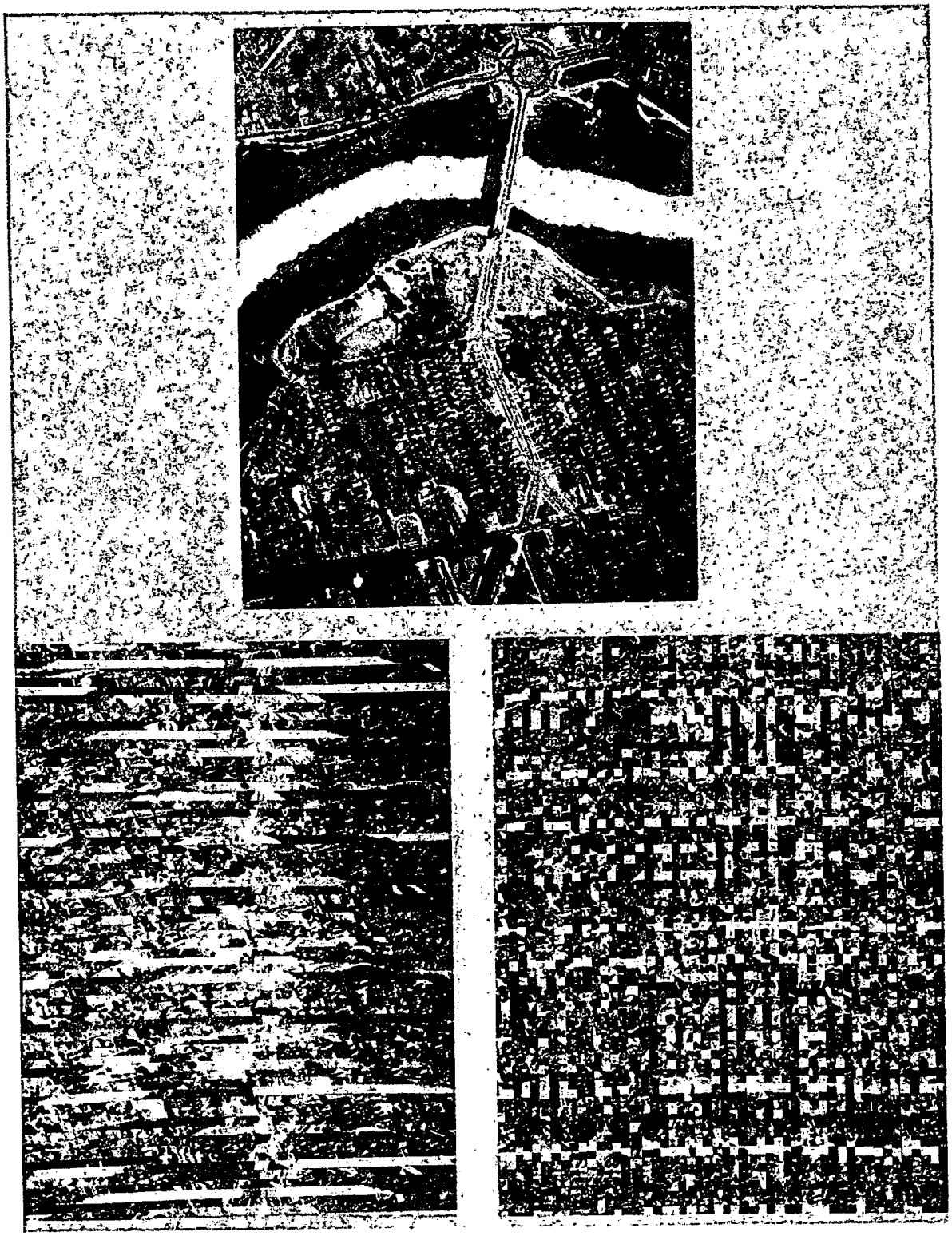


FIGURE 11. Pretransmission coding by single shredding (left) and by double shredding process (right).

SECRET

Phasing is obtained by starting the coding dials at a given setting and time. Synchronization between coding waves at sending and receiving points is obtained from reference pulses transmitted over the circuit. These will require precise frequency standardization.

code remains fixed until the cards are changed.

The receiving decoder is synchronized on a start-stop basis with the commutator of the sending coder by a regularly repeated pulse signal. The code is repeated every ¾ sec so that no long time phasing is needed. The coder

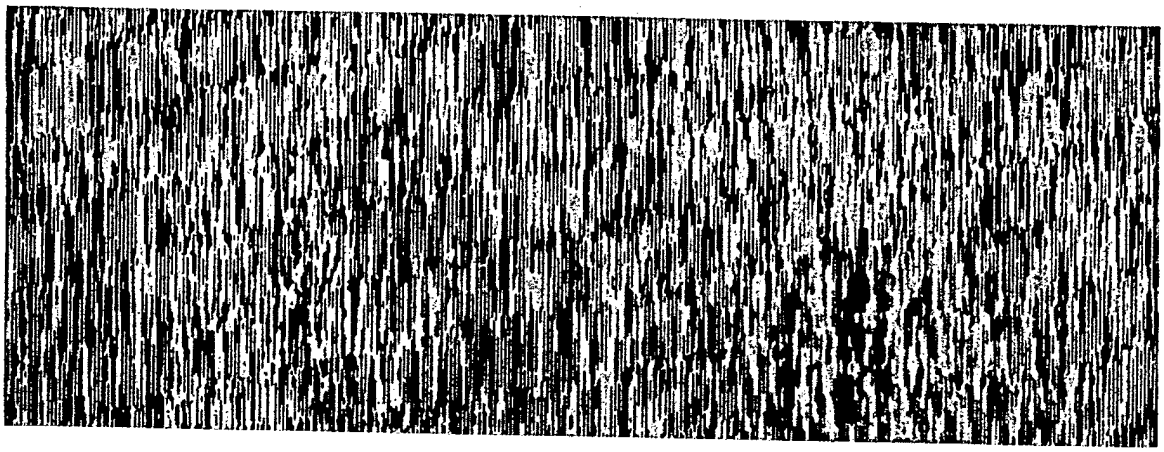


FIGURE 12. Illustration of use of TDS and polarity reversal in combination.

It is probable that multipath propagation will destroy both the coded wave and the synchronizing signal.

The unit as it stands can be used independently for voice or facsimile transmission.

and decoder do not have to be started simultaneously. It is computed that the precision of synchronization required is the same as now obtains on facsimile apparatus. Any skew in the received copy may be corrected by read-

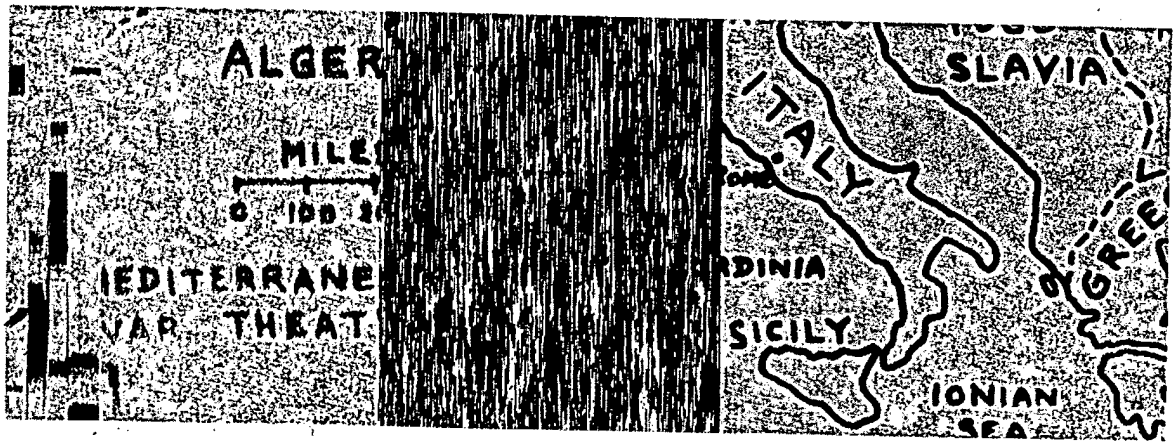



FIGURE 13. Effect of using frequency band transposition [A] and TDS in tandem, thus increasing security offered by either method.

Time delay system [TDS] is represented by the BTL D-Specification model weighing 25 lb, and having a volume of approximately ¾ cu ft. Codes are set up by inserting two perforated cards in their appropriate boxes. A particular

justment of the frequency standards between pictures.

Distortion of the signal by multipath should be the same on TDS as on straight uncoded transmission. At the time of the project, D-Spec

TDS was available privacy equipment, an independent unit, equally applicable to voice or facsimile.

Variable speed [VS] and continuously variable speed [CVS] consists of deviating the drum speed with respect to normal speed at a coded rate, either in fixed steps or continuously to a maximum of ±15 per cent. The apparatus added to a normal facsimile station will depend upon the type of drum drive circuit being used. It may, or may not, exceed in volume the ¾ cu ft already mentioned for other methods.

A basic synchronization accuracy of 1 part in 100,000 will be required. A differential between this standard and the scanner and recorder must be taken to provide the required percentages, slow or fast. The critical condition is that the sequence of speed variations must be exactly the same at scanner and recorder. This requires that the code sequence at the two points should be started with an estimated error of not more than 0.01 sec.

Radio circuit distortions will have no more effect on VS and CVS than on normal facsimile. They may, however, make it difficult to send the timing signal at the start of each message with the precision necessary to start the codes in phase.

A special design of facsimile machine appears to be the most satisfactory solution for the VS and CVS method. It is consequently not an immediately available privacy system.

Pretransmission method [PT] is indicated to be most useful as *one* of the basic methods of a *tandem combination.* The application greatly simplifies tandem transmission since

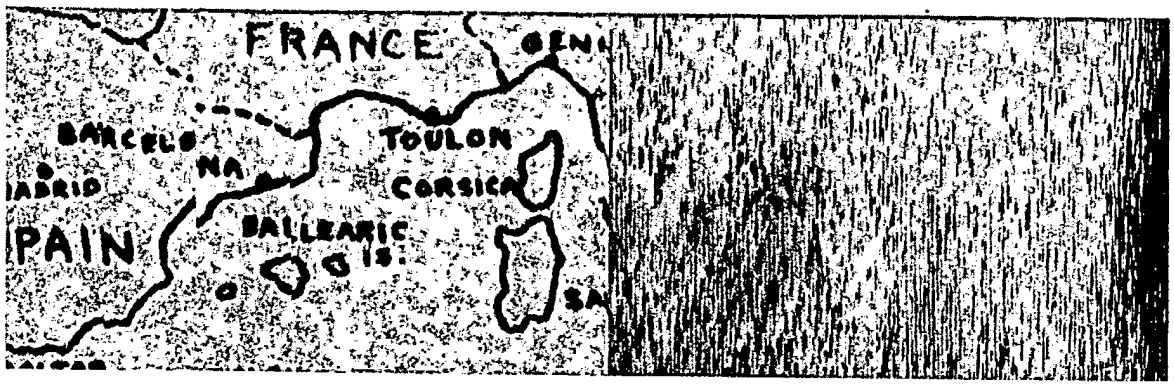



FIGURE 14. Coded and decoded copy produced by combining VS and TDS.

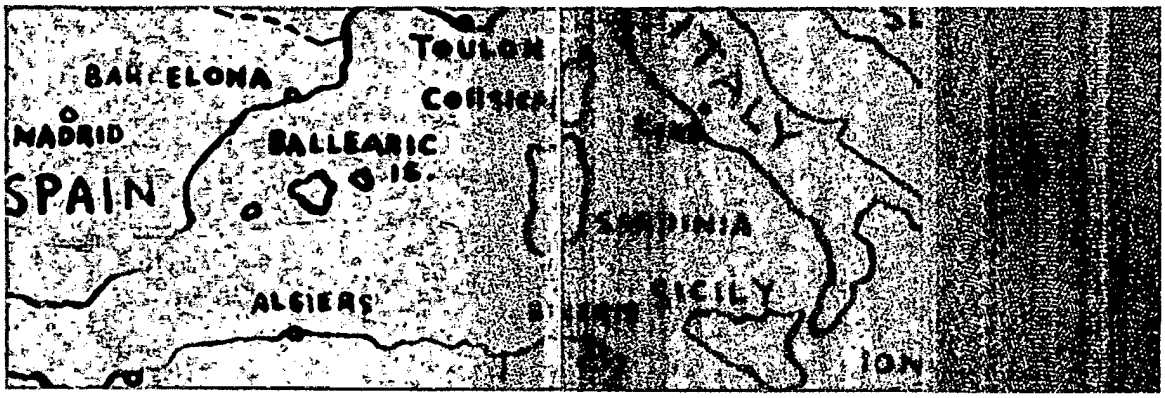



FIGURE 15. Use of frequency multiplication (B) and variable speed (VS) in tandem. Right portion, coded copy; middle portion, decoded copy.

the simultaneous use of more than one set of coders and decoders is not required. The resulting privacy of TDS or VS transmission may thereby be greatly enhanced.

The A-3 graphic method of Faximile, Inc., (Project 13.3-97)[36] and the double shredding method suggested by the Eastman Kodak Company are promising applications of the PT method.

### Summary of Privacy Methods

Several kinds of coding units have been tested which could be built in a volume of 1 cu ft and in mechanical form suitable for military service.

Synchronizing and phasing will be critical problems in radio transmission.

The B system and combinations will not function over radio circuits with severe multipath distortion.

Methods TDS, PR, and VS will not be seriously affected by multipath distortion.

Methods A, B, and TDS can be used ultimately for facsimile and voice coding.

Methods PR and VS are special to facsimile and would be of questionable effectiveness for voice coding.

### Conclusions

In general, privacy systems which are useful for speech may or may not be suitable for facsimile. This is because the original facsimile signal has a regular periodicity which tends to reveal the code that has been applied.

Of the three existing speech privacy systems, A-3 gives no privacy for facsimile transmission whereas TDS and Myopia Mark I are reasonably effective.

The privacy of several variations and combinations of the six basic systems has been estimated in terms of the time required to decode them and will be found in the final report[37] together with proposed methods of decoding and lists of the necessary apparatus.

Much greater privacy is obtained with a tandem combination of two systems than with either system alone.

The best single system so far evaluated (VS) requires three hours for 80 per cent decoding of the picture. It is continuously variable drum speed wherein variations of not less than ±5 per cent occur within each scanning line.

The most effective tandem combination of two systems will apparently require 10 hours to decode 80 per cent of the picture. This is the combination of continuously variable drum speed and D-Specification TDS. Application of CVS with the continuously varying code TDS (C-50) should still further increase the time for decoding. This combination merits investigation.

Pretransmission systems have been proposed during this survey, and have been evaluated. Such systems include coding of the subject copy prior to transmission by normal facsimile means, and decoding of the record copy after it has been received. In general, these methods can effectively code the subject copy but there appear to be technical difficulties in the decoding process.

## 6.3 PRETRANSMISSION FACSIMILE PRIVACY

Project 13.3-97 comprised an investigation of the feasibility of automatically enciphering and deciphering graphic material such as maps, photographs, drawings, etc., by strobotronic photography. The material is scrambled by transposing elementary sections of the graphic original before transmission.

### Basic Method Utilized

Basically the pretransmission scrambling method investigated under this project is equivalent to cutting the copy into vertical strips which are transposed and remounted so that although the information within the strips is in proper order vertically, the picture is mutilated horizontally. After remounting the vertical strips, the resulting copy is cut into strips horizontally and after transposition of the elements, the copy is again assembled. Now, of course, the original information is hidden to a degree depending upon the smallness of the individual elements and the manner in which they are scrambled. Although the feature was not incorporated in the model produced under the instant contract, some of the

elements might be upside down as well as out of order; it is also conceivable that some of the elements might be reversed.

The final product of the several transpositions can be sent to the receiver by courier, by mail, or by wire or radio facsimile or photographic transmission methods.

### The Actual Mechanism

In the machine developed and the model produced, the following sequence of events occurs. The copy to be scrambled is wrapped upon a cylindrical drum and rotated by a motor at a speed which is not critical. A single strip of this copy is illuminated and its image is projected upon a similarly mounted sheet of photographic paper which rotates, not continuously, but in steps.

After the first portion or "frame" of the photographic paper is exposed, the drum carrying the sensitized paper moves one step bringing another frame of the paper into readiness for the second exposure. In the meantime the subject has moved to a new location, according to a key or code, and at the proper time this new portion of the original is photographed upon the sensitive paper. When all portions of the subject strip have been photographed, a new strip of the copy, adjacent to or otherwise with respect to the first strip, would be photographed. In this manner all the copy would be impressed upon the photographic paper but with the elements out of order.

After development, the negative image with vertical elements transposed would be used as an original and a new print made, this time with the scrambling performed in a direction at right angles to the first encipherment. The second print would be a positive like the original material but with all elements out of order.

Increased privacy could be secured by performing another mutilation this time enciphering the transposed copy which is placed on the drum displaced, say, a half-strip in width.

The deciphering is electrically and mechanically the inverse of the operation which scrambles the copy. According to the proper key, portions are photographed upon a sheet of paper which is developed to a negative image. As many copying operations must take place as occurred in scrambling the material in the first place and, of course, the proper key must be used.

### Theory of Operation

Optically it is possible to "stop" the motion of a rapidly moving object at various points in its line of travel if it is illuminated by flashes of light of such short duration that for the period of the flash no appreciable movement of the object occurs.

In the case of the graphic privacy system developed under this project, the moving object is the message to be scrambled. The flashes of light are furnished by the discharge of electrically charged capacitors through gas-filled strobotron tubes. Photographic means are used to record the results.

The original material is scanned through an aperture and by its means and that of a lens system, ½x2-in. sections of the copy are photographed on the sensitive paper rotated by the drum on which it is mounted.

Naturally, the flashes of light must be properly timed in accordance with the relative positions of the two drums and must have the proper intensity. Timing is effected by electronic circuits described in the final report on the project.

Sixteen exposures result in transferring a column 2 in. wide by 8 in. high to the photographic paper in coded random ½x2-in. sections. Thereupon the optical assembly is moved axially and another 2-in. strip is photographed. Naturally, the consecutive sections of the material are not photographed in consecutive position on the sensitive paper, but in some other order determined by the key.

The duration of the flash is about 40 μsec so that the continuously rotated copy is, in effect, stationary during the photographic exposure. The overall effect of two cycles of scrambling is to produce a new positive picture made up of ½-in. squares completely out of place with respect to each other and with respect to the original matter.

### Mechanical Details

The apparatus constructed under the project

was composed of the two drums approximately 4 in. in diameter and 9 in. long, one being rotated at approximately 140 rpm by an electric motor through a 25 to 1 reduction gear and the other rotated in steps by a plunger-type solenoid magnet through a ratchet and pawl mechanism. The optical assembly was composed of two strobotron tubes (Sylvania R-4215) and a projection lens and moved along guide rails between and parallel to the axis of the drums. In the model, coding was accomplished by a switchboard composed of 64 flexible electric cords with phone tip plugs and a like number of tip jacks. Eastman Kodak Aero Enlarging Paper (mapping paper) single weight, No. 2, was used since this material is specially treated to minimize dimensional changes in processing.

The copy drum steps once for every two revolutions of the subject drum. During the alternate revolutions, switching and other mechanical actions take place. In deciphering, the enciphered copy is placed upon the stepping drum, the optical assembly is reversed so that the same key may be used to photographically rearrange the elements in their original order.

## Conclusions

Operating tests of the Model GPM-X1 machine proved the validity of the principles involved and indicated: (1) that in a new model much higher drum speeds could be employed, (2) that it would be advisable to complete the encipherment in a single photographic operation to avoid cumulative errors, (3) that it would be feasible to build a machine that would automatically encipher a clear message in a two-dimensional randomized copy consisting of squares at least as small as 0.2 in. on a side, and (4) that a newly proposed plan for changing keys should be utilized. Such a new machine would provide a substantial term of privacy for graphic copy.

# Chapter 7

# MISCELLANEOUS PROJECTS

THE FINAL TWO PROJECTS considered in this volume are related in a general way to the subject matter that has gone before. Under Project C-52,[a] Division 13 developed a cryptographic rotor which had certain advantages over the similar rotor in use at the time. Project C-71[b] was set up to study the radio transmissions of German submarines in an endeavor to determine if frequency-modulation were being used in addition to the normal amplitude modulation. Methods were developed for recording and studying these signals, the recording apparatus being somewhat similar to the schemes described in the earlier portions of this volume.

## 7.1 ROTOR FOR CRYPTOGRAPHIC USE

Project C-52 was concerned with the design, development, and test of a set of rotors for multiple transposition coding when used on a suitable printer typewriter. Decoding was accomplished by use of a reversing switch.

### STATE OF THE ART

At the time this project was started the Signal Corps had in use a typewriter type of coding and decoding machine which would automatically perform a quadruple transposition ciphering each time a key was struck. This was accomplished by means of four disks (actually rotary switches), each disk having input and output terminals for each letter of the alphabet. The interconnecting wires between these terminals gave the particular transposition for that disk. Four such disks were used in series. After each letter was coded, one or more of these disks was rotated to change the code for the next letter. The machines in use by the Signal Corps had two disadvantages. First, it was quite difficult to rotate the disks since heavy pressures had to be kept on the contact fingers in order that good electrical connections could be made. Second, the construction of the contacts in the disks was such that many troubles were encountered with arcing and tracking across the insulating sectors between contact points. These two difficulties prevented the machines from being used more widely.

### OBJECT OF THE INVESTIGATION

The widespread use of codes and ciphers by the military forces in time of war makes it essential that the process of coding and decoding messages be made as simple as possible. This is usually accomplished by either mechanical or electrical devices or a combination of both. An ideal solution of this problem is a machine with a standard typewriter keyboard upon which a message may be written in plain language resulting in a printed version of this message being coded automatically by the machine and delivered instantaneously. The so-called transposition cipher is most commonly used, in which the letter "a" for instance, when struck on the keyboard, causes some other letter to replace it in the coded message. For purposes of additional security, it is arranged so that the next time the letter "a" is used a different letter represents it than that one which was originally used. A wide variety of multiple transpositions may be used to obtain the necessary security.

Such a transposition can be obtained by having an electrical connection made when a key on the keyboard is depressed. This electrical connection is made to a contact finger which touches one of twenty-six contacts on an insulated rotary disk. On the other side of this disk there are also twenty-six contacts, one for each letter of the alphabet. An electrical connection is permanently made by wires from contacts on one side of the disk to contacts on the other side in a predetermined manner to give the alphabetical transposition which is desired. Twenty-six outgoing contacts bear on

[a] Project C-52, Contract OEMsr-542, Fournier Institute.

[b] Project C-71, Contract OEMsr-880, Western Electric Company, Inc.

each of the rotor contacts and are connected to a printer circuit which causes a letter to be printed corresponding to the contacts through which the electrical circuit was made. Such an arrangement with one rotor disk gives a single alphabetical transposition. A more secure code can be obtained if several transposition disks are used in series, and are rotated in some predetermined fashion to make the breaking of the coded messages even more difficult.

sary to use a rather strong spring on the contact fingers. This made it very difficult to turn the rotors, an operation which was necessary for each new letter which was transmitted. Since these devices were to be used in advanced locations where electric power was not available, it was not possible always to provide some strong solenoid action to force this rotation against the necessary friction. To accomplish this by a straight mechanical linkage to the

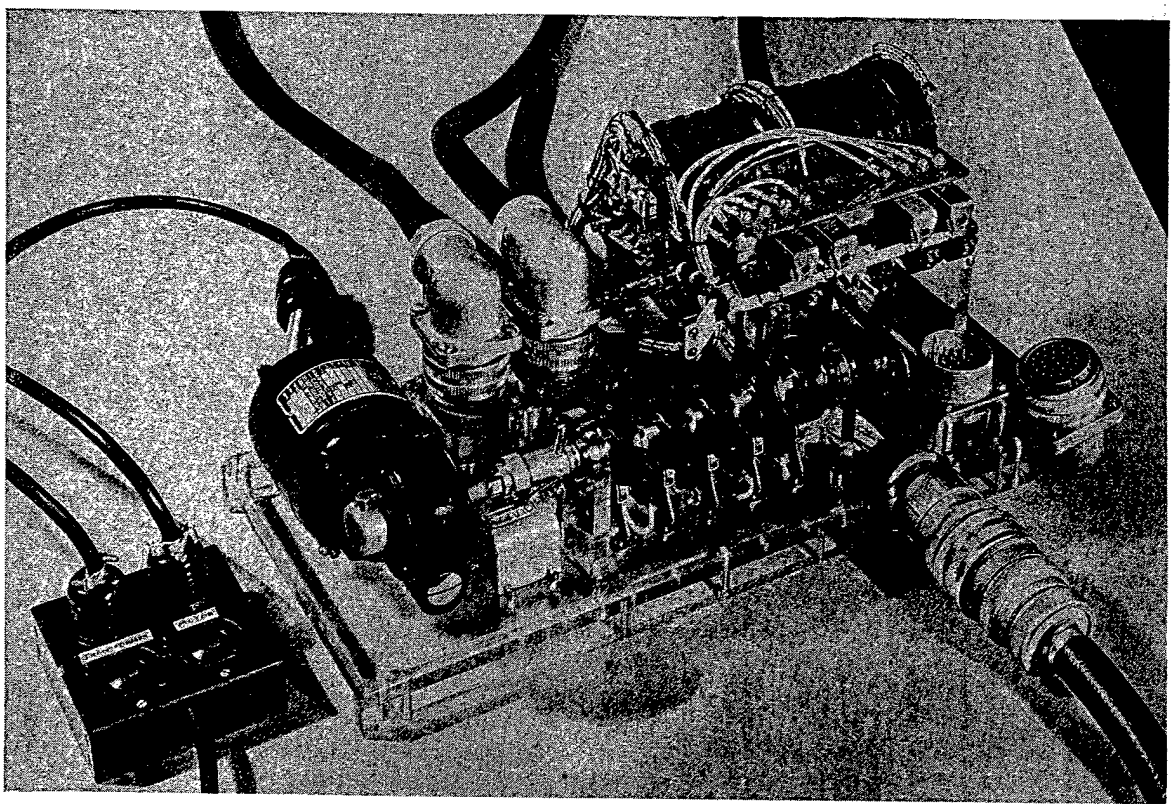


FIGURE 1. General view of testing equipment for cryptographic rotor, rotors in place ready for use.

It is also possible to design an electrical reversing mechanism which enables the same machine to be used in decoding messages. The coded message is transcribed on the keyboard as it was originally received, and the plain test version appears automatically decoded on the printer tape from the machine.

Machines of this description were in use by the Signal Corps at the time of the project, but two difficulties had been encountered. The first difficulty was that to make a reliable contact with the existing designs, it was necessary to use a very special keyboard with a long distance of travel for each key, and would have required the use of considerable force when the key was struck.

A second difficulty was that the existing designs used a bakelite disk in which were molded brass inserts which were turned until they were flush with the bakelite surface. As the disks were rotated after each letter, the contact finger rubbed across the bakelite in its travel from one rotor contact to the adjacent one. This resulted in a track being made across the bake-

lite surface, and ultimately a low-resistance path was built up, which led to electrical breakdown and sparking across this path. When this happened the rotor had to be discarded and a new one substituted.

The object of this investigation was to develop a rotor which could be used in such a device without the difficulties of voltage breakdown between the contacts and excessive mechanical friction during rotation. It was necessary that any proposed rotor be readily manufacturable, and if possible, it was desired to make the connection between the contacts on each side of the rotor sufficiently flexible so that they could be changed readily in the field.

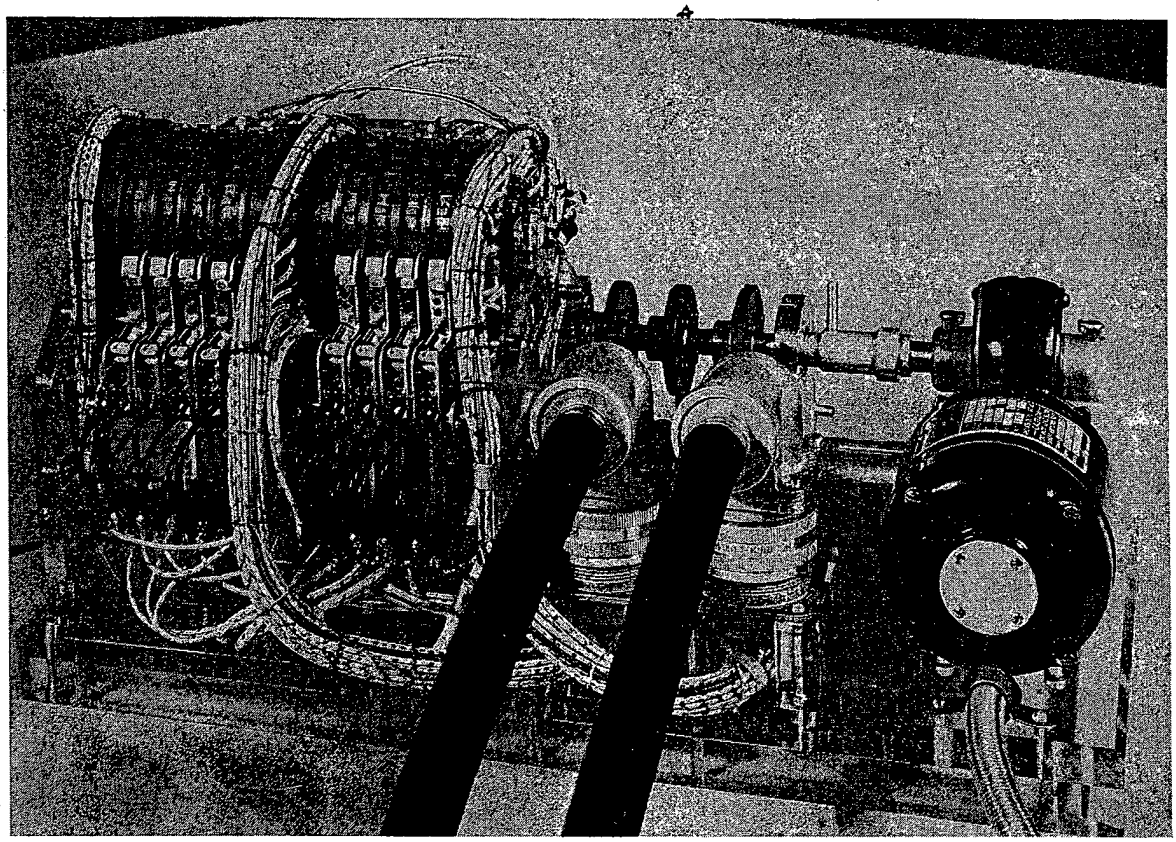


FIGURE 2. Back view showing details of eight rotor disks.

## PROCEDURE

There were two principal problems involved in attacking the project, (1) to design and construct the rotors and contact and (2) to devise proper test equipment to insure that the design would be satisfactory. Two actual rotors were designed and the second which was smaller and less complex than the first was actually constructed and submitted to the Signal Corps. Most of the time and effort were spent on test equipment. After rotors and test equipment had been designed and constructed, life tests were run and demonstrations were made.

The coding disks and rotors constructed were quite easy to rotate while still giving reliable electrical contact as proved by the life tests. Substantially complete freedom from leakage and tracking between terminals and contacts was achieved. The final model should be readily and easily manufactured in large quantities. So far as is known no use was made of the designs or models.

The final report[38] on the project gives complete mechanical description including working drawings.

## 7.2 RADIO RECORDING

Project C-71 comprised an investigation of the possible existence of frequency modulation in certain telegraph transmissions and development of means for recording the transmissions.

### SUMMARY OF THE PROJECT

The work under this project was carried out at the request of the Navy Department as a means of identifying German naval vessels by the characteristics of their telegraph transmitters. Such identification, by recordings, would supplement the direction-finder net set up to watch for enemy signals.

Under the project more than a thousand transmissions were recorded by means of apparatus developed to detect the frequency-modulation in the transmissions and were transmitted to the Navy.

The final report[39] of the project gives the means used and the results obtained.

# BIBLIOGRAPHY

Numbers such as Div 13-302-M3 indicate that the document listed has been microfilmed and that its title appears in the microfilm index printed in a separate volume. For access to the index volume and to the microfilm, consult the Army or Navy agency listed on the reverse of the half-title page.


1. *Speech Privacy Systems, Interception, Diagnosis, Decoding, Evaluation,* OSRD 4573A, Final Report Project C-43, W. Koenig and C. H. G. Gray, BTL, Oct. 12, 1944. Div. 13-302-M3
2. *A Coding Arrangement for C-50 A-3 Privacy System,* J. M. Fraser, OSRD 4573B, Preliminary Report 21 of Part II, Final Report Project C-43, BTL, July 31, 1943. Div. 13-302-M4
3. *Methods for the Automatic Scrambling of Speech,* G. Guanella, OSRD 4573B, Preliminary Report 5 of Part II, Final Report Project C-43, December 1941. Div. 13-302-M4
4. *Methods for the Automatic Scrambling of Speech,* W. Koenig and P. W. Blye, OSRD 4573B, Preliminary Report 5 of Part II, Final Report Project C-43, BTL, December 1941. Div. 13-302-M4
5. *Analysis of Brown Boveri Two-Dimensional Speech Scrambling System,* W. Koenig, OSRD 4573B, Preliminary Report 9 of Part II, Final Report Project C-43, BTL, Sept. 25, 1942. Div. 13-302-M4
6. *"The Carrier Nature of Speech,"* Homer Dudley, *Bell System Technical Journal,* Vol. 19, October 1940, p. 495.
7. *"Remaking Speech,"* Homer Dudley, *Journal Acoustical Society of America,* Vol. 11, October 1939, p. 169.
8. *Speech Privacy Development,* R. K. Potter, OSRD 201, Final Report Project C-1, BTL, June 4, 1941. Div. 13-301.3-M2
9. *Privacy Considerations in Connection with Present and Future TDS Unit Designs and Recommendations for New Models of TDS Privacy Equipment,* R. K. Potter, OSRD 196, Final Report Project C-1A, BTL, May 20, 1941. Div. 13-301.3-M1
10. *Continuously Coded TDS, Speech Privacy Equipment,* Eugene B. Mechling, OSRD 2068, Final Report Project C-50, BTL, Nov. 1, 1943. Div. 13-301.31-M1
11. *Frequency Time Division Speech Privacy System,* L. Schott, OSRD 1725, Final Report Project C-66, BTL, May 29, 1943. Div. 13-301.3-M4
12. *Code Changing Attachment for TDS Speech Privacy Units,* C. W. Carter, OSRD 1541, Final Report Project C-65, BTL, Apr. 30, 1943. Div. 13-301.3-M3
13. *Telegraphy Applied to TDS Speech Privacy Systems,* C. W. Carter, OSRD 1047, Final Report Project C-55, BTL, Oct. 3, 1942. Div. 13-304.3-M1
14. *RCA Speech Secrecy Research,* Project C-54, RCA Laboratories.
    Part I. *Proposed Portable Speech Privacy Unit with High Security,* A. V. Bedford, OSRD 1882, Feb. 2, 1943. Div. 13-301.1-M1
    Part II. *Description of Speech Privacy Unit Model RCAL-1 and Related Information,* A. V. Bedford, OSRD 3107, Oct. 30, 1943. Div. 13-301.1-M2
    Part III. *Modification of Speech Privacy Units, Radio Tests and Conclusions,* A. V. Bedford, OSRD 3395, Feb. 25, 1944. Div. 13-301.1-M3
15. *Speech Secrecy System Development,* O. M. Dunning, OSRD 207, Final Report Project C-15, Hazeltine Service Corp., Oct. 28, 1941. Div. 13-301.2-M1
16. *Variable Band Shift Filter,* D. F. Hoth, OSRD 4573B, Preliminary Report 11 of Part II, Final Report Project C-43, BTL, Nov. 25, 1942. Div. 13-302-M4
17. *Large Spectrograms Made on Variable Area Pattern Machine,* W. Koenig, OSRD 4573B, Preliminary Report 13 of Part II, Final Report Project C-43, BTL, Jan. 13, 1943. Div. 13-302-M4
18. *Method of Finding the Decoding Permutations in Brown Boveri Two-Dimensional Scrambling System,* W. Koenig, OSRD 4573B, Preliminary Report 10 of Part II, Final Report Project C-43, BTL, Oct. 31, 1942. Div. 13-302-M4
19. *Mechanical and Numerical Aids for Cracking Repeated Code TDS,* A. D. Fowler and W. Koenig, OSRD 4573B, Preliminary Report 14 of Part II, Final Report Project C-43, BTL, Jan. 25, 1943. Div. 13-302-M4
20. *Experiments in Cracking Two-Dimensional Scrambles,* W. Koenig, OSRD 4573B, Preliminary Report 22 of Part II, Final Report Project C-43, BTL, July 23, 1943. Div. 13-302-M4
21. *Evaluation of the Privacy Afforded for Non-Repeated Code TDS Systems (C-50 TDS),* W. Koenig, OSRD 4573B, Preliminary Report 26 of Part II, Final Report Project C-43, BTL, Nov. 30, 1943. Div. 13-302-M4
22. *Variable Area Speech Patterns,* W. Koenig, OSRD 4573B, Preliminary Report 1 of Part II, Final Report Project C-43, BTL, May 21, 1942. Div. 13-302-M4
23. *Variable Area Pattern Machine,* D. F. Hoth, OSRD 4573B, Preliminary Report 7 of Part II, Final Report Project C-43, BTL, Sept. 14, 1942. Div. 13-302-M4
24. *Playback Machine for Variable Area Speech Patterns,* W. Koenig, OSRD 4573B, Preliminary Report 12 of Part II, Final Report Project C-43, BTL, Jan. 6, 1943. Div. 13-302-M4
25. *Privacy Evaluation of Repeated Code TDS and A-3 Privacy Equipment in Tandem,* W. Koenig,

OSRD 4573B, Preliminary Report 19 of Part II, Final Report Project C-43, BTL, May 27, 1943. Div. 13-302-M4

26. *Use of Monotone or Whispered Speech on Privacy Systems*, W. Koenig, OSRD 4573B, Preliminary Report 16 of Part II, Final Report Project C-43, BTL, Feb. 25, 1943. Div. 13-302-M4
27. *Evaluation of the Security Afforded by the RCA-Bedford Speech Privacy System*, W. Koenig, OSRD 4573B, Preliminary Report 18 of Part II, Final Report Project C-43, BTL, May 26, 1943. Div. 13-302-M4
28. *Decoding Equipment for TDS, Split Band, and Two-Dimensional Speech Scrambling System*, W. Koenig, OSRD 4573B, Preliminary Report 15 of Part II, Final Report Project C-43, BTL, Jan. 25, 1943. Div. 13-302-M4
29. *Playback Devices for Spectrograms*, L. Y. Lacy, OSRD 4573B, Preliminary Report 17 of Part II, Final Report Project C-43, BTL, Mar. 30, 1943. Div. 13-302-M4
30. *Analysis of Generalized TDS Codes*, A. D. Fowler, OSRD 4573B, Preliminary Report 3 of Part II, Final Report Project C-43, BTL, June 16, 1942. Div. 13-302-M4
31. *Analysis of Self-Converse TDS Codes*, A. D. Fowler, OSRD 4573B, Preliminary Report 6 of Part II, Final Report Project C-43, BTL, Aug. 19, 1942. Div. 13-302-M4
32. *TDS Field Decoding Test at Camp Coles*, W. Koenig and A. E. Ruppel, OSRD 4573B, Preliminary Report 24 of Part II, Final Report Project C-43, BTL, Oct. 19, 1943. Div. 13-302-M4
33. Part II, Final Report on Project C-43, containing all the preliminary reports, most of which are included in this bibliography. Those reports not so included are:

    No. 2. *Results of Experimental Intercept Work at Holmdel, New Jersey and Point Reyes, California*, P. W. Blye and L. Y. Lacy, OSRD 4573B, BTL, May 29, 1942. Div. 13-302-M4

    No. 4 *Sonovox Secrecy System*, L. Y. Lacy, OSRD 4573B, BTL, July 2, 1942. Div. 13-302-M4

    No. 8. *Speech Scrambling System Proposed by Frank D. Lewis*, W. Koenig and P. W. Blye, OSRD 4573B, BTL, Aug. 29, 1942. Div. 13-302-M4

    No. 20. *Speech Privacy and Synchronizing System Devised by Captain Henry P. Hutchinson*, D. O. Slater, OSRD 4573B, BTL, July 31, 1943. Div. 13-302-M4

    No. 23. *Intercept Work at Point Reyes, California*, H. Kahl, OSRD 4573B, BTL, July 26, 1944. Div. 13-302-M4

    No. 25. *Interception of Enemy Radiotelephone Communications Employing Privacy Systems; Problems, Procedures and Tools*, W. Koenig, OSRD 4573B, BTL, Oct. 12, 1943. Div. 13-302-M4
34. *Speech Privacy Problems*, A. D. Fowler, OSRD 5686, Final Report Project 13-106, BTL, Aug. 18, 1945. Div. 13-300-M1
35. *Spectrographs for Field Decoding Work*, C. H. G. Gray, OSRD 3824, Final Report on Project 13.3-86, BTL, May 31, 1944. Div. 13-302.1-M3
36. *Facsimile Privacy*, H. H. Beverage, OSRD 1881, Final Report Project C-73, RCA Laboratories, June 7, 1943. Div. 13-303-M1

    Abridged Report, OSRD 2005, Oct. 15, 1943. Div. 13-303-M2
37. *Investigation of Pre-Transmission Facsimile Privacy Methods*, J. V. L. Hogan, OSRD 6346, Final Report Project 13.3-97, Faximile, Inc., June 30, 1945. Div. 13-303-M3
38. *Development of a Rotor for Cryptographic Use*, Harner Selvidge, OSRD 1607, Final Report Project C-52, Fournier Institute, May 1, 1943. Div. 13-304.1-M1
39. *Radio Recording*, A. M. Curtis, Final Report Project C-71, BTL, June 15, 1943. Div. 13-304.2-M1
40. *Control Circuits for the Sound Spectrograph*, W. Koenig, OSRD 4573B, Preliminary Report 27 of Part II, Final Report Project C-43, BTL, Apr. 29, 1944. Div. 13-302-M4
41. *The Sound Spectrograph, A Time-Frequency-Intensity Analyzer*, W. Koenig, Preliminary Report Project C-43, BTL, Oct. 1, 1943. Div. 13-302.1-M2
42. *Operating Notes for Spectrograph Model Nos. 2 and 3*, R. G. McCurdy, Project C-43, BTL, Jan. 30, 1943. Div. 13-302.1-M1
43. *Notes on Description and Operation of Special Speech Privacy Decoding Equipment Used at Point Reyes, California*, O. M. Akey and H. Kahl, Project C-43, BTL, June 30, 1944. Div. 13-302-M2
44. *Speech Privacy Decoding*, OSRD 386, Final Report Project C-32, BTL, Jan. 31, 1942. Div. 13-302-M1
45. *Interception of Enemy Radiotelephone Communications Employing Privacy Systems; Problems, Procedures and Tools*, W. Koenig, OSRD 4573B, Preliminary Report 25 of Part II, Final Report Project C-43, BTL, Oct. 12, 1943. Div. 13-302-M4
46. *Results of Experimental Intercept Work at Holmdel, New Jersey and Point Reyes, California*, P. W. Blye and L. Y. Lacy, OSRD 4573B, Preliminary Report 2 of Part II, Final Report Project C-43, May 29, 1942. Div. 13-302-M4
47. *Intercept Work at Point Reyes, California*, H. Kahl, OSRD 4573B, Preliminary Report 23 of Part II, Final Report Project C-43, BTL, July 26, 1944. Div. 13-302-M4
48. *Memo of Changes in Speech Privacy Units as Released to the Army by RCA Laboratories*, A. V. Bedford, Project C-54, RCA, Oct. 19, 1944. Div. 13-301.1-M4

# OSRD APPOINTEES

## DIVISION 13

*Chief*

C. B. JOLLIFFE (December 1942 to May 1945)
HARADEN PRATT (May 1945 to May 1946)

*Deputy Chief*

K. C. BLACK

*Technical Aides*

J. L. ALLISON
C. F. DALZIEL
J. F. MCCLEAN
A. F. MURRAY

*Members*

K. C. BLACK
O. E. BUCKLEY
J. H. DELLINGER
W. L. EVERITT
G. C. FICK
R. H. GEORGE
C. H. G. GRAY
A. HAZELTINE
J. A. HUTCHINSON
C. M. JANSKY
L. F. JONES
D. G. LITTLE
R. K. POTTER
H. PRATT
C. A. PRIEST
F. M. RYAN

*Section Heads*

| | | |
|---|---|---|
| Section 13.1 | Direction Finding | L. F. JONES |
| Section 13.2 | Radio Propagation Problems | J. H. DELLINGER |
| Section 13.3 | Speech Secrecy | R. K. POTTER |
| Section 13.4 | Special Communications Problems | C. A. PRIEST |
| Section 13.5 | Precipitation Static | H. PRATT |
| Section 13.6 | Miscellaneous Projects | D. G. LITTLE |

*Consultants*

L. V. BERKNER
H. H. BEVERAGE
E. D. BLODGETT
D. G. LITTLE
R. K. POTTER

*Interference Reduction Committee*

K. C. BLACK
H. D. DOOLITTLE
R. G. FLUHARTY
A. HAZELTINE
J. C. R. LICKLIDER
C. T. MORGAN
A. F. MURRAY
S. S. STEVENS
O. W. TOWNER

CONTRACT NUMBERS, CONTRACTORS, AND SUBJECT OF CONTRACTS FOR DIVISION 13

| *Contract Number* | *Name and Address of Contractor* | *Subject* | *Refer to Chapters* |
|---|---|---|---|
| NDCrc-125 | Western Electric Company, Inc. New York, N. Y. | Speech secrecy system. | 2 |
| NDCrc-196 | Western Electric Company, Inc. New York, N. Y. | Continuation of speech secrecy system. | 2 |
| NDCrc-139 | Hazeltine Service Corporation New York, N. Y. | Hazeltine speech secrecy system. | 3 |
| OEMsr-230 | Western Electric Company, Inc. New York, N. Y. | Decoding speech codes. | 4 |
| OEMsr-435 | Western Electric Company, Inc. New York, N. Y. | Continuation of decoding speech codes. | 1, 3, 4 |
| OEMsr-490 | Western Electric Company, Inc. New York, N. Y. | Improved speech secrecy. | 2, 6 |
| OEMsr-542 | Fournier Institute Lemont, Ill. | Development of rotor for cryptographic use. | 6 |
| OEMsr-592 | Radio Corporation of America Camden, N. J. | Speech secrecy research. | 3, 5, 6 |
| OEMsr-628 | Western Electric Company, Inc. New York, N. Y. | Telegraphy applied to TDS speech secrecy system. | 2 |
| OEMsr-782 | Western Electric Company, Inc. New York, N. Y. | Code changing attachment for TDS speech privacy unit. | 2 |
| OEMsr-795 | Western Electric Company, Inc. New York, N. Y. | Frequency-time division speech analyzer. | 2 |
| OEMsr-880 | Western Electric Company, Inc. New York, N. Y. | Radio recording. | 6 |
| OEMsr-837 | Radio Corporation of America Camden, N. J. | Facsimile secrecy. | 6 |
| OEMsr-1110 | Western Electric Company, Inc. New York, N. Y. | Spectrographs for field decoding work. | 5 |
| OEMsr-1202 | Faximile, Inc. New York, N. Y. | Graphic privacy system. | 6 |
| OEMsr-1440 | Western Electric Company, Inc. New York, N. Y. | Speech privacy problems. | 5 |

## SERVICE PROJECT NUMBERS

The projects listed below were transmitted to the Executive Secretary, NDRC, from the War or Navy Department through either the War Department Liaison Officer for NDRC or the Office of Research and Inventions (formerly the Coordinator of Research and Development), Navy Department.

| *Service Project Number* | *Subject* | *Refer to Chapters* |
|---|---|---|
| SC-12 | Speech secrecy system. | 2 |
| SC-12 | Continuation of speech secrecy system. | 2 |
| SC-12 | Hazeltine speech secrecy system. | 3 |
| SC-12 | Improved speech secrecy. | 2, 6 |
| SC-12 | Speech secrecy research. | 3, 5, 6 |
| SC-12 | Code changing attachment for TDS speech secrecy system. | 2 |
| SC-12 | Frequency-time division speech analyzer. | 2 |
| SC-19 | Telegraphy applied to TDS speech secrecy system. | 2 |
| SC-25 | Development of rotor for cryptographic use. | 6 |
| SC-28 | Decoding speech codes. | 4 |
| SC-28 | Continuation of decoding speech codes. | 1, 3, 4 |
| SC-43 | Facsimile secrecy. | 6 |
| NS-130 | Radio recording. | 6 |
| NS-134 | Graphic privacy system. | 6 |
| NS-349 | Speech privacy problems. | 5 |

# INDEX

The subject indexes of all STR volumes are combined in a master index printed in a separate volume. For access to the index volume consult the Army or Navy Agency listed on the reverse of the half-title page.