Cracking the Courtyard Crypto

By David D. Stein

I looked down at the large number of yellow pages littering the top of my desk, obscuring its dark oak finish. Each page was covered in hundreds of alphabetic letters that, although they appeared to be arranged randomly, were really carefully laid out in ordered columns. For the past week or so I had been feeling that I was very close to a solution--But was I? As a hobby, I had solved many puzzles since I was a child, and I had discovered that the most difficult challenge was continually dealing with the nagging fear that I may be on the wrong track. The voice in my head would whisper, "Maybe you're mistaken--maybe this first part of the Kryptos code is really not a polyalphabetic Vigenere Tableau after all--maybe it's a different type of code entirely. Or maybe it is a Vigenere code, but it's been double or triple encoded--or maybe it was encoded backwards, or maybe..."

This is the worst train of thought an amateur cryptanalyst can have--it goes nowhere, and it is tempting to give in to frustration at the seemingly infinite number of possible solutions and abandon the effort. So as I had done dozens of times before, I pushed these thoughts away and pressed on. The thing to do, I told myself again and again, was simply to stick to what I knew to be the facts. Let the encoded text itself guide me, and keep speculation to an absolute minimum. I should follow my instincts occasionally, but then remember to always keep track of my assumptions and be prepared to revise my thinking if a hunch doesn't work out.

And suddenly it happened--I was hit by that sweetly ecstatic, rare experience that has been described as a "moment of clarity". All of the doubts and speculations about the thousands of possible alternate paths simply melted away, and I clearly saw the one correct course laid out in front of me. Taking a fresh sheet of yellow paper I slowly and deliberately wrote out a new column of letters, followed by another, and then another. I continued this for several pages, then computed mathematically which rows were most likely to represent the correct plaintext letters, and searched for logical combinations between adjacent letters. I tried to contain my excitement as I witnessed the miracle of the letters slowly forming together into words, one after the other. Within the next few hours I had finished. After more than seven years and some 400 hours of laboring over piles and piles of paper covered with gibberish, I was at last looking down at a paragraph of clear English text. I had broken out the first part of the Kryptos code.

Introduction

I don't remember the first time I saw, or even heard about, the Kryptos sculpture in the courtyard. But when I did finally notice the huge, curved copper plates with their mysterious perforated inscription, I decided I would give their decryption a try. I have always been interested in puzzles, and I became fascinated with the thought of that encoded message standing quietly in the headquarters' courtyard year after year, taunting everyone to try to read its hidden message. After working on the code for a while, I learned that the basic problem-solving techniques that I needed for decryption were not so very different from those that I used in my work as a technical analyst. And in my reading I also learned something else; that although codebreaking is a fascinating hobby, it's more than just fun and games--throughout history, lives literally have been lost and saved due to cryptanalysis.

Ever since I initially began sharing with people the progress I had made deciphering the code covering the Kryptos sculpture, I have had the interesting experience of being inundated with questions about it. By far the most frequent question asked is "How much did you get paid for solving that thing?" (Many people seemed to think that there was some kind of prize involved). The next most common question is "How long did it take you to solve it?" Notwithstanding my wife's riposte ("so long, that it almost wasn't worth it"), this question is more difficult. I was not keeping track of the time, and in any event, I was not in any hurry to solve the puzzle. Codebreaking for me is a hobby--if it stops being fun and begins to seem more like work, then it's time to quit and start doing something else. My best estimate of roughly 400 hours seems about right, had I been working continuously. I don't know how long it would have taken me if I had been trying to solve it as fast as possible, though. I had expected the most prevalent question to be "What does the message say?"; however, this one only made it into third place, followed closely by (humorously I hope) "Don't you have anything better to do with your time?". Although I'm not sure just how to respond to this last one, I do like to talk about the progress I've made on the Kryptos problem. However, I must confess that I sometimes feel a little uncomfortable revealing the message without having an opportunity to provide a full explanation.

There are several reasons that I don't like to just blurt out the solution to the Kryptos puzzle. First, it is important to remember that the message is still incomplete--I have not yet broken out the last 97 characters of the 866 character inscription. Second, as will be seen, the message is enigmatic and open to interpretation. Finally, I believe that simply presenting the solution without showing the methodology behind it is cheating people a little. The creators of Kryptos no doubt intended to inspire people to try to solve it for themselves. Simply showing the "solution" that I have derived steals away a little of the excitement and appreciation of the problem, and can discourage people from trying their own interpretations.

However, when asked to write an article for "Studies in Intelligence", I became intrigued by the idea of trying to explain what can be a complicated and convoluted subject in a manner that hopefully could be understood by anyone. After it was suggested to me that it could well be impossible to explain the methodology concisely and in a non-technical manner, I couldn't resist taking up the challenge.

Where to Begin?

When first confronted with the coded full text of the Kryptos sculpture, the task of deciphering it can seem formidable--even impossible. Where to begin? Even the most casual of observations reveals that the writing on the sculpture is divided into 2 main pieces. One side (figure 1) depicts a somewhat modified "Vigenere Tableau" (a series of alphabets used for the coding and decoding of text); the other side contains the actual coded message of 866 characters interspersed with four "question marks" (figure 2).

One method for deciphering a code begins by counting up the number of times that each letter of the alphabet occurs throughout the message--a so-called "frequency count". However, it seemed reasonable to me that different sections of the Kryptos code may have been enciphered with different coding schemes; if so, it would be necessary to perform frequency counts on each part separately. Looking through the code, I seemed to see

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
A	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P
B	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T
C	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O
D	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S
E	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A
F	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B
G	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C
H	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D
I	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E
J	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F
K	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G
L	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H
M	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I
N	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J
O	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L
P	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M
Q	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N
R	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q
S	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U
T	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V
U	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W
V	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X
W	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z
X	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K
Y	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R
Z	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y

Figure 1. One Side of "Kryptos" Sculpture, Depicting Vigenere Tableau

```
E M U F P H Z L R F A X Y U S D J K Z L D K R N S H G N F I V J
Y Q T Q U X Q B Q V Y U V L L T R E V J Y Q T M K Y R D M F D
V F P J U D E E H Z W E T Z Y V G W H K K Q E T G F Q J N C E
G G W H K K ? D Q M C P F Q Z D Q M M I A G P F X H Q R L G
T I M V M Z J A N Q L V K Q E D A G D V F R P J U N G E U N A
Q Z G Z L E C G Y U X U E E N J T B J L B Q C R T B J D F H R R
Y I Z E T K Z E M V D U F K S J H K F W H K U W Q L S Z F T I
H H D D D U V H ? D W K B F U F P W N T D F I Y C U Q Z E R E
E V L D K F E Z M O Q Q J L T T U G S Y Q P F E U N L A V I D X
F L G G T E Z ? F K Z B S F D Q V G O G I P U F X H H D R K F
F H Q N T G P U A E C N U V P D J M Q C L Q U M U N E D F Q
E L Z Z V R R G K F F V O E E X B D M V P N F Q X E Z L G R E
D N Q F M P N Z G L F L P M R J Q Y A L M G N U V P D X V K P
D Q U M E B E D M H D A F M J G Z N U P L G E W J L L A E T G
E N D Y A H R O H N L S R H E O C P T E O I B I D Y S H N A I A
C H T N R E Y U L D S L L S L L N O H S N O S M R W X M N I
T P R N G A T I H N R A R P E S L N N E L E B L P I I A C A E
W M T W N D I T I E E N R A H C T E N E U D R E T N H A E O E
T F O L S E D T I W E N H A E I O Y T E Y Q H E E N C T A Y C R
E I F T B R S P A M H N E W E N A T A M A T E G Y E E R L B
T E E F O A S F I O T U E T U A E O T O A R M A E E R T N R T I
B S E D D N I A A H T T M S T E W P I E R O A G R I E W F E B
A E C T D D H I L C E I H S I T E G O E A O S D D R Y D L O R I T
R K L M L E H A G T D H A R D P N E O H M G F M F E U H E
E C D M R I P F E I M E H N L S S T T R T V D O H W ? O B K R
U O X O G H U L B S O L I F B B W F L R V Q Q P R N G K S S O
T W T Q S J Q S S E K Z Z W A T J K L U D I A W I N F B N Y P
V T T M Z F P K W G D K Z X T J C D I G K U H U A U E K C A R
```

Figure 2. Opposite Side of "Kryptos" Sculpture, Containing the Coded Message

different patterns throughout, but I wanted to quantify these impressions. Therefore just as a starting point, I decided to count up the number of times each letter in figure 2 occurred in each row of the message. By plotting these counts as a function of row for each letter of the alphabet (26 plots in all), I would be able to watch how often each letter was being used as the message evolved. In particular, if the count stayed approximately constant for a number of rows, this would indicate the same type of code was being used for that part of the message.

A typical example of one of the 26 plots, for encoded letter "J", is shown in figure 3. (Of course, these "J"s are not really "J"s at all, but are ciphertext letters representing plaintext letters of the alphabet.)

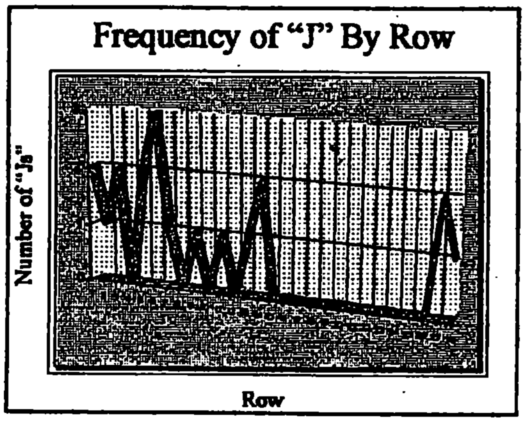


Figure 3. Frequency of "J" Occurrences by Row

It can be seen that the letter "J" occurred 2 times in the first row of the Kryptos message, 1 time in the second row, and so on. I noted that there was a marked change in letter frequency occurring between rows 14 and 15; that is, from row 1 to 14 there were J's appearing in almost every row, but from row 15 to row 25 there were no J's appearing at all. It will be shown later on exactly what is causing this phenomenon; the important point to me was that I saw a good indication that rows 1-14 were encoded with a different type of code than rows 15 and beyond. (There was also an indication that the last 2 or 3 rows were encoded with a different type of code than the preceding rows.) The dramatic change from row 14 to 15 was seen in virtually all of the 26 frequency plots; two more examples are shown below in figures 4 and 5 (for letters "Q" and "K", respectively).

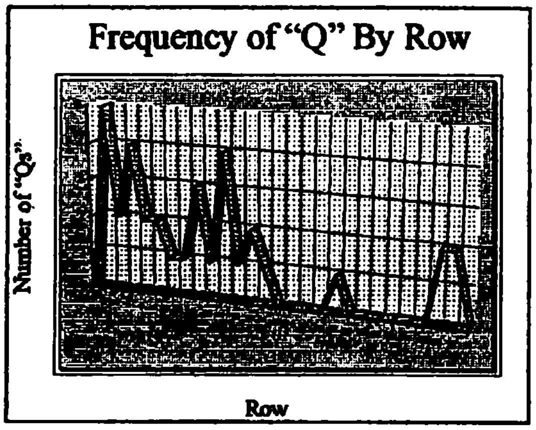


Figure 4. Frequency of "Q" By Row

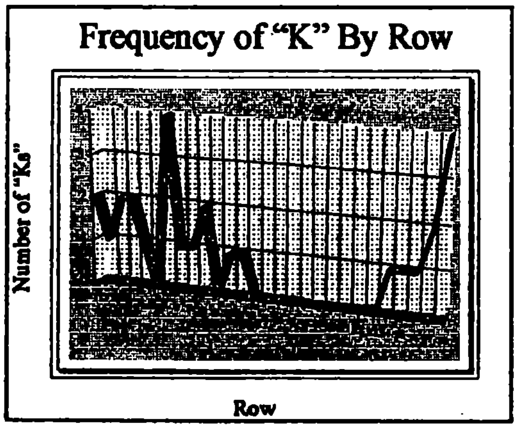
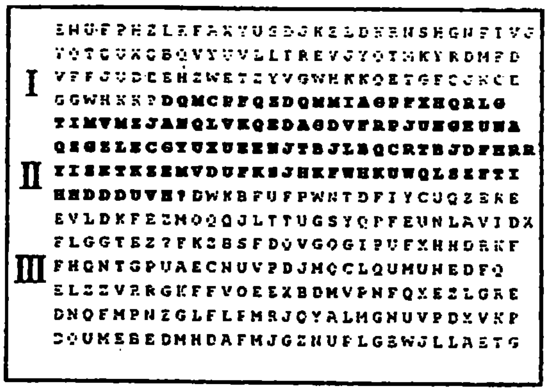


Figure 5. Frequency of "K" By Row

Based on these results, I therefore divided the code into 2 sections; rows 1-14 were designated the "top" section, and rows 15-28 the "bottom". I then further divided the top section into 3 parts using the four question marks as the dividing points; I designated these portions as Parts I, II, and III respectively (figure 6). I began my attempts at deciphering with the 125 characters of Part II because this piece looked more interesting to me than the other two parts.



```
  EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJ
  YQTQUXQBQVYUVLLTREVJYQTMKYRDMFD
I VFPJUDEEHZWETZYVGWHKKQETGFQJNCE
  GGWHKK?DQMCPFQZDQMMIAGPFXHQRLG
  TIMVMZJANQLVKQEDAGDVFRPJUNGEUNA
  QZGZLECGYUXUEENJTBJLBQCRTBJDFHRR
II YIZETKZEMVDUFKSJHKFWHKUWQLSZFTI
  HHDDDUVH?DWKBFUFPWNTDFIYCUQZERE
  EVLDKFEZMOQQJLTTUGSYQPFEUNLAVIDX
  FLGGTEZ?FKZBSFDQVGOGIPUFXHHDRKF
III FHQNTGPUAECNUVPDJMQCLQUMUNEDFQ
  ELZZVRRGKFFVOEEXBDMVPNFQXEZLGRE
  DNQFMPNZGLFLPMRJQYALMGNUVPDXVKP
  DQUMEBEDMHDAFMJGZNUPLGEWJLLAETG
```

Figure 6. Top Section of Kryptos Code, Divided into 3 Parts

Encryption Schemes

Encryption schemes are methods of changing an original plaintext message into a coded one. Although there are many different types of encryption methods, virtually all of them fall into two main categories: substitution codes and transpositional codes.

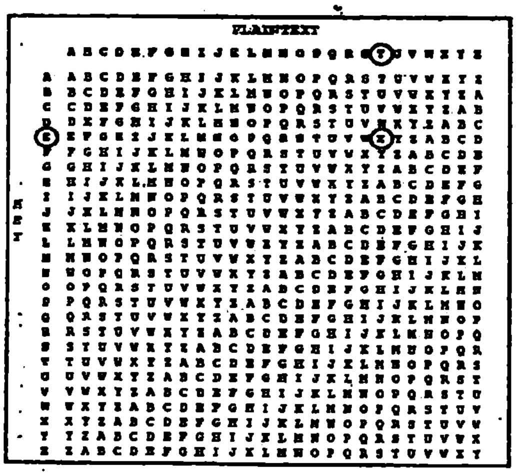
very interesting concept!

Substitution Codes: Each letter of the plaintext message is changed into another letter of the alphabet. In a simple, monoalphabetic substitution (i.e. using a single alphabet), a particular letter will be encoded by the same letter every time it is used.

Example:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	m	**e**	**r**	**i**	**t**	**a**	**b**	**c**	**d**	**f**	**g**	**h**	**j**	**k**	**l**	**n**	**o**	**p**	**q**	**s**	**u**	**v**	**w**	**x**	**y**	**z**

So **"The Red Badge of Courage"** would be encoded: ***"sct pti emibt la rlupmbt"*** using the keyword "merit".

However, if a polyalphabetic substitution is used (i.e. one using multiple alphabets), then a plaintext letter can be encoded by a number of different letters. One common polyalphabetic method is the so-called "Vigenere Tableau".



PLAINTEXT

KEY

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Example:																			
	Key:	A	B	L	E	A	B	L	E	A	B	L	E	A	B	L	E	A	B
	Plaintext:	W	h	a	t	h	a	t	h	G	o	d	W	r	o	u	g	h	t
	Ciphertext:	***w***	***i***	***l***	***x***	***h***	***b***	***e***	***l***	***g***	***p***	***o***	***a***	***r***	***p***	***f***	***k***	***h***	***u***

Note plaintext "W" stays "W" in the first occurrence, but changes into "A" in the second.

Transposition Codes: All of the letters used in the coded message are exactly the same as those used in the plaintext, but they are arranged in a different order.

Frequency Counts

The frequency count is one of the cryptanalyst's most powerful tools. By computing how often each letter appears throughout the message, it is possible to determine important clues about the code employed. In figure 7 is plotted a typical frequency count of normal English text.

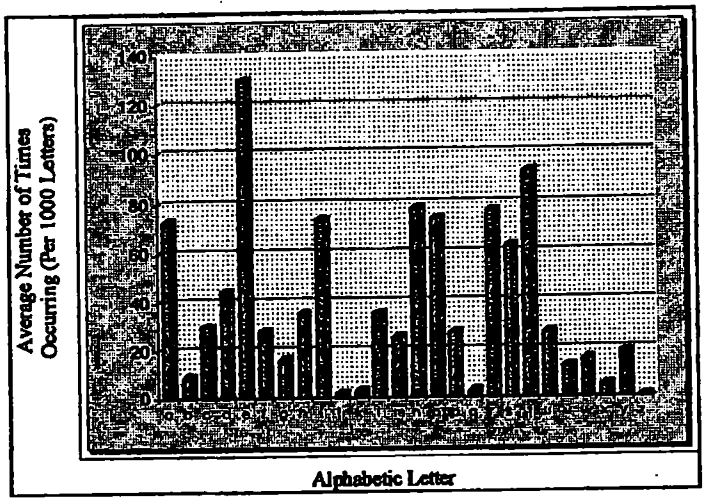


Figure 7. Normal Frequency Distribution for the English Language

Each bin represents the number of times that that letter occurs, on the average, for every 1000 letters encountered. For example, as you are reading these lines, the words I am using are unavoidably being constructed of letters that comprise such a distribution. So tenaciously does this pattern adhere to our language that it is virtually impossible to write or speak without it betraying its presence. And even if one were to artificially construct a few sentences or paragraphs that do not follow this distribution, it would turn out to be so contrived that new patterns would inevitably develop. So because it is an essential and unavoidable part of our language, from a cryptanalytical point-of-view, the pattern is also a code's greatest weakness.

In figure 8 a frequency count for Part II of the Kryptos code is plotted. It was easily seen, from comparison with figure 7, that the pattern was very different from the normal distribution for English.

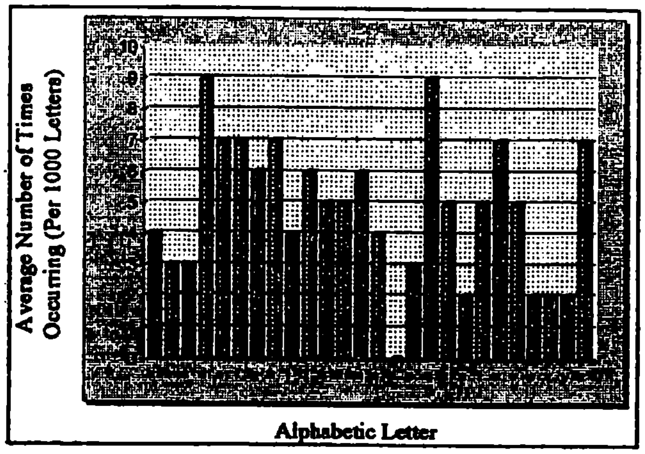


Figure 8. Frequency Count for Part II of Kryptos Code

In particular, the distribution appeared much flatter. This is exactly what I would expect to see for a polyalphabetic substitution code, where the distributions for several different alphabets would tend to "average out" when combined. Because the modified Vigenere Tableau—a polyalphabetic substitution code—is inscribed on the Kryptos sculpture, it made sense to try this first as a working hypothesis for this part of the code.

Finding the Length of the Key Word

A common method for breaking a Vigenere code involves first determining the length of the keyword that was used to encipher the message. The code can then be broken up into its constituent single alphabets (or "monoalphabets") and then analysis can be performed on each cipher alphabet to determine to which Vigenere alphabet it corresponds. Once these Vigenere alphabets are determined, the code can be easily deciphered. Note that nowhere in this analysis is it necessary to actually resolve the content of the keyword.

In order to ascertain the length of the keyword used in Part II of the cipher, I needed to make use of a cryptanalytical tool known as the "index of coincidence", or I.C. This concept conveys the probability that, given a distribution of letters, any two of them chosen at random will be the same. The details are covered in the field of statistics, and they are not significant here; the formula and an example calculation is provided, (see box), if anyone wants to repeat the analysis for themselves. The important point is that for any set of letters, the average value of the I.C. will range from 0.38 up to 0.66. The closer this average value is to 0.38, the more likely it is that the set of letters is completely random. If the value is closer to 0.66, then it is more likely that the letters represent a monoalphabet.

I first divided the text of Part II into 2 single alphabets and computed the average I.C., then divided the text into 3 alphabets and again computed the average I.C., then divided into 4 alphabets, and so on. Finally, I plotted each average I.C. as a function of the number of alphabets (figure 9).

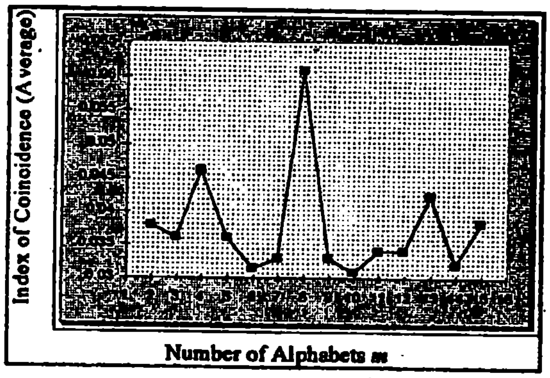


Figure 9. I.C. vs. Number of Alphabets for Part II

1	2	3	4	5	6	7	8
D	Q	M	C	P	F	Q	Z
D	Q	M	M	I	A	G	P
F	X	H	Q	R	L	G	T
I	M	V	M	Z	J	A	N
Q	L	V	K	Q	E	D	A
G	D	V	F	R	P	J	U
N	G	E	U	N	A	Q	Z
G	Z	L	E	C	G	Y	U
X	U	E	E	N	J	T	B
J	L	B	Q	C	R	T	B
J	D	F	H	R	R	Y	I
Z	E	T	K	Z	E	M	V
D	U	F	K	S	J	H	K
F	W	H	K	U	W	Q	L
S	Z	E	T	I	H	H	D
D	D	U	V	H	?		

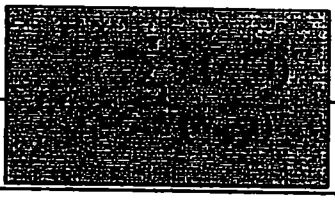
Figure 10. Part II of Kryptos Code Divided into 8 Alphabets

It is easy to see from this figure that the correct key length for this piece of code should be 8 since that number yields an average I.C. value of almost 0.063; thus, I knew that I needed to divide the code into 8 separate alphabets. (figure 10)

Example Computation of I.C. for 7 Alphabets (Kryptos Code Part II)

0.038

Completely Random Letters



0.066

Mono-alphabet

f=letter frequency, N=number of letters in column

1	2	3	4	5	6	7
D	Q	M	C	P	F	Q
Z	D	Q	M	M	I	A
G	P	F	X	H	Q	R
L	G	T	I	M	V	M
Z	J	A	N	Q	L	V
K	Q	E	D	A	G	D
V	F	R	P	J	U	N
G	E	U	N	A	Q	Z
G	Z	L	E	C	G	Y
U	X	U	E	E	N	J
T	B	J	L	B	Q	C
R	T	B	J	D	F	H
R	R	Y	I	Z	E	T
K	Z	E	M	V	D	U
F	K	S	J	H	K	F
W	H	K	U	W	Q	L
S	Z	F	T	I	H	H
D	D	D	U	V	H	

	1	2	3	4	5	6	7
A	0	0	1	0	2	0	1
B	0	1	1	0	1	0	0
C	0	0	0	1	1	0	1
D	2	2	1	1	1	1	1
E	0	1	2	2	1	1	0
F	1	1	2	0	0	2	1
G	3	1	0	0	0	2	0
H	0	1	0	0	2	2	2
I	0	0	0	2	1	1	0
J	0	1	1	2	1	0	1
K	2	1	1	0	0	1	0
L	1	0	1	1	0	1	1
M	0	0	1	2	2	0	1
N	0	0	0	2	0	1	1
O	0	0	0	0	0	0	0
P	0	1	0	1	1	0	0
Q	0	2	1	0	1	4	1
R	2	1	1	0	0	0	1
S	1	0	1	0	0	0	0
T	1	1	1	1	0	0	1
U	1	0	2	2	0	1	1
V	1	0	0	0	2	1	1
W	1	0	0	0	1	0	0
X	0	1	0	1	0	0	0
Y	0	0	1	0	0	0	1
Z	2	3	0	0	1	0	1

Alphabet 1: [2(1)+3(2)+2(1)+2(1)+2(1)]/(18)(17)=0.046
Alphabet 2: [2(1)+2(1)+3(2)]/(18)(17)=0.033
Alphabet 3: [2(1)+2(1)+2(1)]/(18)(17)=0.020
Alphabet 4: [2(1)+2(1)+2(1)+2(1)+2(1)+2(1)]/(18)(17)=0.040
Alphabet 5: [2(1)+2(1)+2(1)+2(1)]/(18)(17)= 0.026
Alphabet 6: [2(1)+2(1)+2(1)+4(3)]/(18)(17)=0.059
Alphabet 7: [2(1)]/(17)(16)=0.007

AVERAGE I.C.:
0.046+0.033+0.020+0.040+0.026+0.059+0.007]/7
= 0.033

Which Vigenere Alphabets to Use?

Now that I had the code divided into 8 monoalphabets, I needed to determine which Vigenere alphabet corresponded to each of them. If the text of Part II had been much longer, the analysis would have been fairly straightforward; I could simply have performed a frequency count for each column and matched the resulting distributions to the English frequency count in figure x. The letter occurring most frequently would most likely have corresponded to plaintext "E", and, since the Vigenere alphabets have a fixed order (cyclical permutation), the identities of the other letters could then have been found. However, from the example presented in figure 11 (for the first column), it is obvious how impossible this method would be for the present problem:

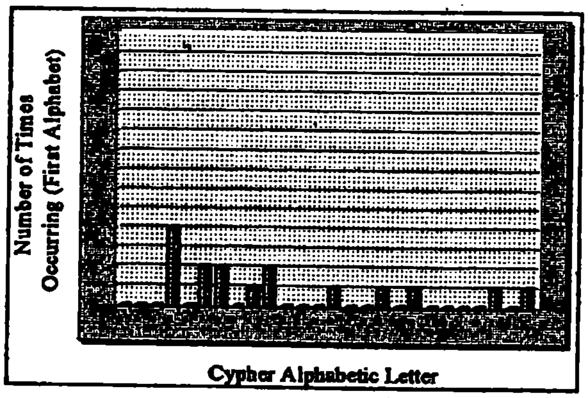


Figure 11. Frequency Count for First Alphabet of Part II

With only around 15 letters available per alphabet, there are simply not enough to determine any kind of alphabetic structure such as that seen in figure 7. So now what?

I must admit that I got stuck at this point for a long time. No doubt a professional cryptanalyst would know several ways to proceed, but I was unsure. And then one day– February 21, 1998 to be exact, I had a breakthrough. How well I remember sitting at my desk, with the sun coming through the window and the birds chirping loudly outside. I don't know if it was divinely inspired (it certainly felt that way), or if simply all of the knowledge that I had gained about the Kryptos code from hundreds of hours of work came together and combined with what I had learned from all of the books I had read on cryptography. In any event, everything suddenly seemed so very clear that I didn't have the slightest doubt about how to proceed, and I was confident that it would work.

This is what I did: Once again I divided the message into 8 separate alphabets. Now, what had become plain to me was that if I wrote out one of the columns along with every possible permutation for each letter in that column, then exactly one of these would contain the true plaintext letters. True, the message would be sampled by every 8 letters, but I could write out the permutations for every column and then look for likely letter combinations among the plaintext (figure 12).

```
D E F G H I J L M N Q U V W X Z K R Y P T O S A B
D E F G H I J L M N Q U V W X Z K R Y P T O S A B
F G H I J L M N Q U V W X Z K R Y P T O S A B C D
I J L M N Q U V W X Z K R Y P T O S A B C D E F G
Q U V W X Z K R Y P T O S A B C D E F G H I J L M
G H I J L M N Q U V W X Z K R Y P T O S A B C D E
N Q U V W X Z K R Y P T O S A B C D E F G H I J L
G H I J L M N Q U V W X Z K R Y P T O S A B C D E
X Z K R Y P T O S A B C D E F G H I J L M N Q U V
J L M N Q U V W X Z K R Y P T O S A B C D E F G H
J L M N Q U V W X Z K R Y P T O S A B C D E F G H
Z K R Y P T O S A B C D E F G H I J L M N Q U V W
D E F G H I J L M N Q U V W X Z K R Y P T O S A B
F G H I J L M N Q U V W X Z K R Y P T O S A B C D
S A B C D E F G H I J L M N Q U V W X Z K R Y P T
D E F G H I J L M N Q U V W X Z K R Y P T O S A B
```

Figure 12. First Column of Part II With Every Possible Permutation

One of these columns must correspond to the correct plaintext letters for the first column of the message in figure 10, but which one?

D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C
D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C
F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E
I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H
Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N
G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F
N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M
G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F
X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W
J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I
J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I
Z	K	R	Y	P	T	O	S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X
D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C
F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C	D	E
S	A	B	C	D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O
D	E	F	G	H	I	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S	A	B	C

Fig. 13. Permutations of First Column, with Uncommon Letters in Red

Looking across the columns (figure 13), it can be seen that some appear more promising than others; those that contain a large number of uncommon letters, for instance (remember, these should now represent actual plaintext letters.) But this all seemed so subjective--and how could I tell which column was the best choice? Columns 1, 5, 7, 11, 15, and 16 each contain at least 5 uncommon letters--very unlikely to occur in such a short message of only 125 characters, so I could rule these out. But what about the others? Column 18, for example, contains 4 "R"s, which is a very common letter, and only 1 "J" (an uncommon letter.) But is that column more likely to represent the plaintext letters than column 22, which has 2 "E"s and 4 "O"s, and no "K"s, "J"s, or "Z"s at all?

What I needed to do was to quantify these observations mathematically. One way to do this would be, for each column, to add up the normal English frequency count associated with each letter. Then the columns with the highest sums would be the best candidates to correspond with the true plaintext letters. Starting with column 1 for example, it can be seen from figure 7 that letter "D" occurs 4.4 times (on the average) for every 100 letters in English, "F" occurs 2.8 times, "I" 7.4 times, and so on. I could have simply summed these up; however, in my studies I learned that it is actually better to compute the sum of the logarithm of the frequencies instead. Thus for the first column, log (4.4) + log (4.4) + log (3.8) + log (7.4) + ...=7.3. One advantage of using the log of the values rather than just the values themselves is that the overall sums will be "penalized" for containing the uncommon letters B, J, K, Q, X and Z; i.e. those with negative log frequency values, and will more dramatically reduce the overall score. The final log sums for each column are presented in figure 14 (the table has been turned sideways for ease of presentation; the rows should correspond to the columns of figure 13.)

D	D	F	I	Q	G	N	G	X	J	J	Z	D	F	S	D	7.3
E	E	G	J	U	H	Q	H	Z	L	L	K	E	G	A	E	13.0
F	F	H	L	V	I	U	I	K	M	M	R	F	H	B	V	16.3
G	G	I	M	W	J	V	J	R	N	N	Y	G	I	C	G	12.8
H	H	J	N	X	L	W	L	Y	Q	Q	P	H	J	D	H	6.4
I	I	L	Q	Z	M	X	M	P	U	U	T	I	L	E	I	16.2
J	J	M	U	K	N	Z	N	T	V	V	O	J	M	F	J	2.9
L	L	N	V	R	Q	K	Q	O	W	W	S	L	N	G	L	12.8
M	M	Q	W	Y	U	R	U	S	X	X	A	M	Q	H	M	10.1
N	N	U	X	P	V	Y	V	A	Z	Z	B	N	U	I	N	11.4
Q	Q	V	Z	T	W	P	W	B	K	K	C	Q	V	J	Q	-5.6
U	U	W	K	O	X	T	X	C	R	R	D	U	W	L	U	14.8
V	V	X	R	S	Z	O	Z	D	Y	Y	E	V	X	M	V	7.3
W	W	Z	Y	A	K	S	K	E	P	P	F	W	Z	N	W	7.0
X	X	K	P	B	R	A	R	F	T	T	G	X	K	Q	X	7.0
Z	Z	R	T	C	Y	B	Y	G	O	O	H	Z	R	U	Z	6.9
R	R	P	S	E	T	D	T	I	A	A	J	R	P	W	R	25.2
Y	Y	T	A	F	O	E	O	J	B	B	L	Y	T	X	Y	16.1
P	P	O	B	G	S	F	S	L	C	C	M	P	O	Z	P	15.6
T	T	S	C	H	A	G	A	M	D	D	N	T	S	K	T	23.7
O	O	A	D	I	B	H	B	N	E	E	Q	O	A	R	O	24.8
S	S	B	E	J	C	I	C	Q	F	F	U	S	B	Y	S	15.4
A	A	C	F	L	D	J	D	W	G	G	V	A	C	P	A	17.4
B	B	D	G	M	E	L	E	V	H	H	W	B	D	T	B	16.2
C	C	E	H	N	F	M	F	W	I	I	X	C	E	O	C	21.9

Figure 14. Log Sum Frequencies for Each Column Permutation

Again, the details of these calculations are not really important--the main point is that the rows in figure 14 with the highest values are the most likely to correspond to the correct plaintext letters.

Finally, Words Start to Appear

It is easy to see from figure 14 that the three highest log sum values correspond to the "R" row (log sum=25.2), the "T" row (log sum=23.7), and the "O" (log sum=24.8). These three values are significantly higher than any of the others. Now, I often imagine a professional cryptographer with a bag of special tools, not unlike a consummate locksmith or doctor, but consisting of alphabetic letter tables and charts rather than picks or scalpels. The English language frequency chart and the I.C. were such tools, and now another one comes into play: namely, the frequency table of initial letters common in English language words. In other words, how likely is it for a particular letter to begin a word. It so happens that the letter "O" occurs as an initial letter an average of about 7.2 times per 100 words, and the letter "R" only about 3.1 times. However, since the letter "T" occurs a whopping average of 16 times per 100 words, this is clearly a good letter to try first.

Knowing that one of the most common words in English is the word "THE", and given that the first letter of Part II could very well be a "T", I naturally wanted to see what would happen if "H" were the second letter and "E" the third. But once I chose these letters, I would then be committed to using all of the other letters in those rows as well. The permutations with log sums for the second and third columns of figure 10 are presented in figures 15 and 16, respectively.

```
Q Q X M L D G Z U L D E U W Z D
U U Z N M E H K V M E F V X K E
V V K Q N F I R W N F G W Z R F
W W R U Q G J Y X Q G H X K Y G
X X Y V U H L P Z U H I Z R P H
Z Z P W V I M T K V I J K Y T I
K K T X W J N O R W J L R P O J
R R O Z X L Q S Y X L M Y T S L
Y Y S K Z M U A P Z M N P O A M
P P A R K N V B T K N Q T S B N
T T B Y R Q W C O R Q U O A C Q
O O C P Y U X D S Y U V S B D U
S S D T P V Z E A P V W A C E V
A A E O T W K F B T W X B D F W
B B F S O X R G C O X Z C E G X
C C G A S Z Y H D S Z K D F H Z
D D H B A K P I E A K R E G I K
E E I C B R T J F B R Y F H J R
F F J D C Y O L G C Y P G I L Y
G G L E D P S M H D P T H J M P
H H M F E T A N I E T O I L N T 29.4
I I N G F O B Q J F O S J M Q O
J J Q H G S C U L G S A L N U S
L L U I H A D V M H A B M Q V A
M M V J I B E W N I B C N U W B
N N W L J C D X Q J C D Q V X C
```

Figures 15. Probable Plaintext for 2nd Column

```
M M H V V V E L E B F T F H F U
N N I W W W F M F C G O G I G V
Q Q J X X X G N G D H S H J H W
U U L Z Z Z H Q H E I A I L I X
V V M K K K I U I F J B J M J Z
W W N R R R J V J G L C L N L K
X X Q Y Y Y L W L H M D M Q M R
Z Z U P P P M X M I N E N U N Y
K K V T T T N Z N J Q F Q V Q P
R R W O O O Q K Q L U G U W U T
Y Y X S S S U R U M V H V X V O
P P Z A A A V Y V N W I W Z W S
T T K B B B W P W Q X J X K X A
O O R C C C X T X U Z L Z R Z B
S S Y D D D Z O Z V K M K Y K C
A A P E E E K S K W R N R P R D
B B T F F F R A R X Y Q Y T Y E
C C O G G G Y B Y Z P U P O P F
D D S H H H P C P K T V T S T G
E E A I I I T D T R O W O A O H  30.5
F F B J J J O E O Y S X S B S I
G G C L L L S F S P A Z A C A J
H H D M M M A G A T B K B D B L
I I E N N N B H B O C R C E C M
J J F Q Q Q C I C S D Y D F D N
L L G U U U D J D A E P E G E Q
```

Figure 16. Probable Plaintext for 3rd Column

It was seen that the log sum frequency for the "H" row of figure 14 is 29.4, and for the "E" row of figure 16 is 30.5—certainly strong values, indicating that these rows are good candidates for being the correct plaintext letters. More importantly, when these three alphabets are lined up, no obvious impossible combinations were seen (figure 17):

```
1 2 3 4 5 6 7 8
T H E
T H E
S M A
C F I
H E I
A T I
G A T
A N D
M I T
D E R
D T O
N O W
T I O
S L A
K N O
T T H
```

Figure 17. Probable Plaintext for First 3 Columns of Part II

What I was looking for here were contradictions--that is, combination of letters that would not be possible in English, such as "AAA" or a "Q" that was not followed by the mandatory "U", for instance. Much to my delight, not only were no contradictions found, there were even heartening signs showing I was definitely on the right track. The word "AND" appeared in row 8, and an indication of the suffix "-TION" started to peek out from row 13. Best of all, that "KNO" in the 15th row was an unexpected gift, since I knew the odds were extremely good that there must be a "W" following it. So all I needed to do to find the next plaintext column was to write out the permutations for the fourth column of figure 14, find the permutation set that contained a "w" in the 15th position, and add this column to figure 17.

Now that I was looking for logical words, calculating the log sum frequencies was no longer necessary--I just had to pick out the one row in each set of permutations that best fit with the already-selected columns of figure 17. What a treat not to have to add up any more of those log frequencies! (I had done so many of these that, at one point, I had memorized all of the letter frequencies and proudly showed off this "skill" to my very patient family, friends and co-workers.) Continuing on in this manner, finding the remaining letters for columns 5-8 was not difficult, and the final plaintext of Part II fell into place:

1	2	3	4	5	6	7	8
T	H	E	Y	U	S	E	D
T	H	E	E	A	R	T	H
S	M	A	G	N	E	T	I
C	F	I	E	L	D	X	T
H	E	I	N	F	O	R	M
A	T	I	O	N	W	A	S
G	A	T	H	E	R	E	D
A	N	D	T	R	A	N	S
M	I	T	T	E	D	U	N
D	E	R	G	R	U	U	N
D	T	O	A	N	U	N	K
N	O	W	N	L	O	C	A
T	I	O	N	X	D	O	E
S	L	A	N	G	L	E	Y
K	N	O	W	A	B	O	U
T	T	H	I	S	?		

Figure 18. Plaintext for All 8 Columns of Part II

I noticed a few surprises. First, the letter "X" seemed to be serving as a punctuation mark in the fourth and 13th rows--probably a period. That could have confused the decryption if it had occurred in the first few columns, but luckily it didn't. Secondly, I now saw that the first word was not "THE" after all, but "THEY". This was another bit of luck (or serendipity), since my initial assumption was wrong but it still led to the right answer. Finally, I noticed that the spelling of "underground" in the 10th row was "incorrect". I was so disconcerted by this that I made one of my rare trips (only about my third) out to the Kryptos sculpture to double check my copy. I actually put my hand out to feel the letter and confirm that I had it correct. But I hesitated to call it an error--it was possible that it could also have been a purposeful effort by code's author to provide a clue for interpreting a deeper part of the solution.

The next thing I did was to look at Part III of the code to see if it was encoded in the same way as Part II. I simply continued out the permutations from figures 14-16 so as to include the letters from Part III. Surprisingly, I quickly found readable plaintext forming from Part III, showing that what I was calling "Parts II and III" were really a single portion of code with a single encryption scheme. Although I wasn't expecting this to be the case, it was a pleasant shock to get the remainder of the message with almost no additional work.

When I tried to decode Part I using the same scheme, however, I found that it did not work. Part I was definitely encrypted differently than the rest of the top section, so I had to start all over again, first computing the I.C.s under the assumption (which proved correct) that I was once more working with a Vigenere cipher for this part:

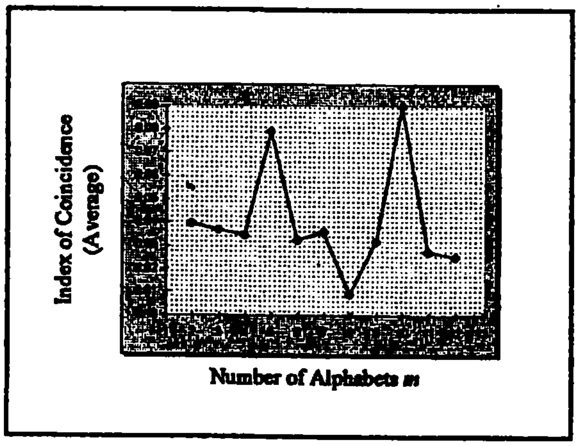


Figure 19. I.C. vs. Number of Alphabets for Part I

Although the graph was cruder than for Part II because it was obtained from a fewer number of letters (note that some of the I.C.s seem to exceed the theoretical limit of 0.063), it was still obvious that a key length either 5 or 10 was being employed. (These multiple high I.C. values were the result of the way the I.C.s were calculated. Since high I.C. values are caused by letter repetitions within a column, columns split up into multiples of the keylength (i.e. 5, 10, 15, etc.) will show up as additional peaks at these values.) I tried both, but it was 10 that proved to crack this part. I performed the same analysis as just shown previously for Parts II and III, and the final decryption for the entire top half of the code is presented here:

```
BETWEEN SUBTLE SHADING AND THE ABSENCE OF
LIGHT LIES THE NUANCE OF ILLUSION. THEY
USED THE EARTH'S MAGNETIC FIELD. THE
INFORMATION WAS GATHERED AND TRANSMITTED
UNDERGROUND TO AN UNKNOWN LOCATION.  DOES
LANGLEY KNOW ABOUT THIS? THEY SHOULD ITS
BURIED OUT THERE SOMEWHERE. WHO KNOWS ITS
EXACT LOCATION? ONLY WW. THIS WAS HIS
LAST MESSAGE. THIRTY-EIGHT DEGREES FIFTY-
SEVEN MINUTES SIX POINT FIVE SECONDS
NORTH SEVENTY-SEVEN DEGREES EIGHT MINUTES
FORTY-FOUR SECONDS WEST ID BY ROWS.
```

Figure 20. Completed Plaintext for Top Section of Kryptos Code

So What Does the Bottom Section Say?

Of course, all the time that I was working away at the top section of the Kryptos code, I would take occasional breaks to look at the bottom section as well. I saw almost immediately that this section, like the top, was made up of different parts. From the frequency by row charts (figures 3-5), there was a strong hint that the last three lines or so were encoded with a different scheme than the rest. So I decided to divide the bottom section into two parts at the question mark, and called them Parts IV and V.

```
  ENDYAHROHNLSRHEOCPTEOIBIDYSHNAIA
  CHTNREYULDSLLSLLNOHSNOSMRWXMNI
IVTPRNGATIHNRARPESLNNELEBLPIIACAE
  WMTWNDITIEENRAHCTENEUDRETNHAEOE
  TFOLSEDTIWENHAEIOYTEYQHEENCTAYCR
  EIFTBRSPAMHNEWENATAMATEGYEERLB
  TEEFOASFIOTUETUAEOTOARMAEERTNRTI
  BSEDDNIAAHTTMSTEWPIEROAGRIEWFEB
  AECTDDHILCEIHSITEGOEAOSDDRYDLORIT
  RKLMLEHAGTDHARDPNEOHMGFMFEUHE
  ECDMRIPFEIMEHNLSSTTRTVDOHW?OBKR
  UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
 VTWTQSJQSSEKZZWATJKLUDIAWINFBNYP
  VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR
```

Figure 21. Encoded Bottom Section of Kryptos Code

Starting with Part IV, the first thing I did was call out my faithful old friend, the frequency count:

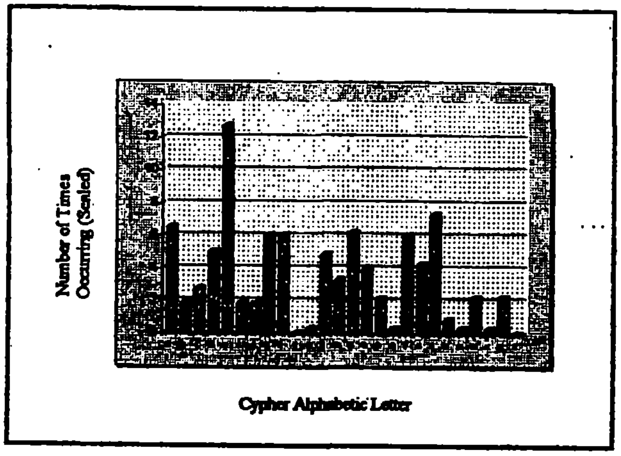
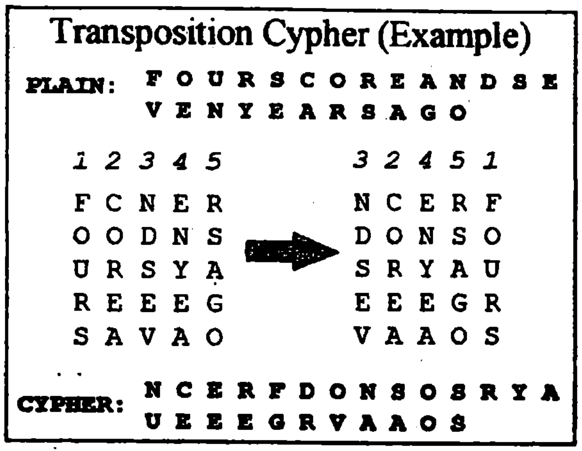


Figure 22. Frequency Count for Part IV

Comparing this chart to figure 7, it was obvious that the letters in Part IV were occurring with the same frequency as they occur in normal English. This implied that this part of the code must be encoded with a transposition code (see box.) Interesting...the Kryptos code (so far) seemed to be encoded with the two most fundamental types of codes--the substitution and the transpositional.

Because Part IV was probably a transpositional code, I knew that all of the 336 letters were already in plaintext, but I needed to determine their correct ordering. At first it seemed like an impossible task, with an almost infinite number of possibilities. After reading up on the subject, however, I soon realized that there are standard ways to encrypt a transpositional code, just as there were for the substitution codes. And I had a hunch that the code's author may have used one of the most fundamental types of encryption.



Transposition Cypher (Example)

```
PLAIN:  F O U R S C O R E A N D S E
        V E N Y E A R S A G O

   1 2 3 4 5          3 2 4 5 1

   F C N E R          N C E R F
   O O D N S          D O N S O
   U R S Y A          S R Y A U
   R E E E G          E E E G R
   S A V A O          V A A O S

CYPHER: N C E R F D O N S O S R Y A
        U E E E G R V A A O S
```

Figure 23. Example of a Basic Substitution Code

In a basic substitution code, the plaintext message usually is first written out vertically in matrix form, with a certain number of columns and rows; it may or may not be a square matrix (see figure 23). The columns are then mixed around, and the new ciphertext is read horizontally from the rows. To decipher the message, the reverse procedure must be carried out.

Defining the Problem

In order to read the Kryptos transpositional message, then, the first thing that I needed to do was to determine the basic structure of the array; that is, ascertain into how many columns and rows the 336 letters were divided. For example, one solution might be to try 18 columns by 36 rows, since 18 times 36 equals 336. Another solution could be 56 columns by 6 rows. But the array does not need to be completely filled in--it could be, for example, a 17 x 20 grid, but with only 13 letters in the final row. So how would I know the right choice?

The big breakthrough took place when I realized that there were really only a finite number of possible solutions. I thought about the problem this way: suppose I looked at something a little more simple, say a transpositional message of only 29 characters (figure

24). Now, since I had constructed this problem myself and therefore knew the answer, it was easy to see the methodology required to solve it.

```
       B            B            B-1
 I W R R O T  W E E U C N  S I O D N
 N T N F I T  O H T O S E

  1 2 3 4 5        4 5 2 1 3

  I W S N O        N O W I S
  W E I T H        T H E W I
  R E O N T        N T E R O
  R U D F O        F O U R D
  O C N I S        I S C O N
  T N   T E        T E N T

 N O W I S T H E W I N T E R
 O F O U R D I S C O N T E N
 T
```

Figure 24. A Simple Substitution Code With Array Not Completely Filled In

Now I imagined how things would look if I only had the ciphertext, without any clues on how to solve it. I would first need to figure out how many rows and columns there should be, decide how to break up the original message into "pieces" (i.e. columns) of a certain length (call this length "B"), and then figure out how many letters should be in each piece. Once this was known, I would have to assemble the columns into the correct order before I could read the plaintext.

Looking at figure 24, it is apparent that, when the array is not completely filled in, there can only be pieces of length B or B-1, since the shorter words will always be just one letter shorter than the longer ones needed to fill in the array. Gradually, I realized that the mathematical relation should be as follows (defining A=B-1):

$$Ax + By = 29,$$

$$\text{or } y=(29-Ax)/B$$

where x is number of pieces of length A and y is the number of pieces of length B. Since x and y must be integers, (pieces cannot consist of fractions of a letter), the condition that there are only a finite number of solutions is forced. So for a given A and B, only certain y values are possible for each x. For example, if A=4 and B=5:

X	*Y*
0	5.80
1	**5.00**
2	4.20
3	3.40
4	2.60
5	1.80
6	**1.00**
7	0.20

Since y must be a positive integer, there are only 2 possible values for x for this example: 1 and 6.

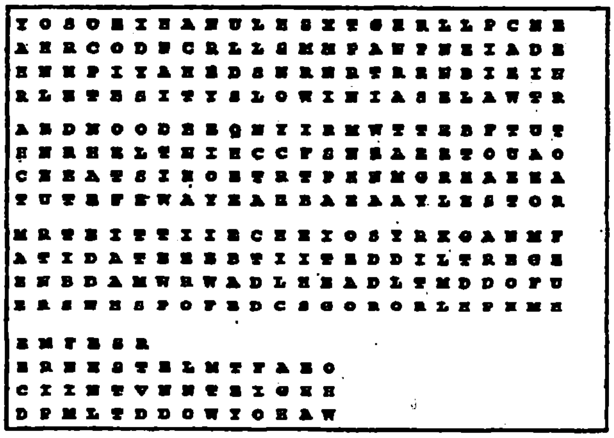
Now I was ready to try my model on the actual Kryptos code. Substituting the number of characters in Part IV into the previous formula,

$$y=336-Ax/B$$

I could now determine how many pieces of length A and B were possible to fit into the 336 characters inscribed on this part of the sculpture. I had noted that Part IV began with the word "END". This could be only a coincidence, but I wondered if it could be a hint by the code's author that maybe this word represented the final column in the grid. If true, this would imply either a grid made up mostly of columns of length 3 and 4, or else a grid made up all of column length 3. From working with the code for so long, I had gradually developed the strong feeling that the matrix was not very square at all--that is, it consisted of only a few very long rows. It is always difficult to describe hunches, but, in this case, my feelings were based on the realization that once the columns were finally assembled, they would need to be reordered into columns to make horizontal words. And when I tried possible solutions using long columns, I found so many contradictions that I was forced to conclude that the columns couldn't be very long.

Finding the Columns

So after many months of trying different ideas, I finally decided to try A=3 and B=4 as a working hypothesis. But I still needed to know how many words of length 3 and how many of length 4 there were. From symmetry, I had the feeling that the final three letters in Part IV represented a three letter word, since I had hypothesized that the first three letters did. From the previous formula, I knew that there were only certain solutions that were allowable--(x=0, y=84), (x=4, y=81), (x=8, y=78)...all the way up to (x=112, y=0). That's still 28 different solutions to check, but fortunately the correct choice of (x=8, y=78) was one of the first that I considered:



```
Y O S O E I H A N U L E S I T G E R L L P C N E
A H R C O D N C R L L S M N F A N Y N E I A D E
H N N P I Y A N E D S N R N R T R E N B I E I N
R L E T E S I T Y S L O W I N I A S E L A W T R

A E D N O O D E E Q N Y I R M W T T E B F T U T
H N R H E L T H I E C C F S N E A E E T O U A O
C E E A T S I N O E T R T P E N M G R E A E E A
T U T E F E W A Y E A E B A E A A Y L E S T O R

M R T E I T T I I E C H E Y O S Y R K G A N M F
A T I D A T E E E B T I I T E D D I L T R E G E
E N B D A M W R W A D L H E A D L T M D D O F U
E R S N H S P O F E D C S G O R O R L H P I M H

E M F E S R
E R N E S T E L M T F A E O
C I I N T V N N T E I G E H
D P M L T D D O W Y O E A W
```

Figure 25. Correct (But Unordered) Column Arrangement for Part IV

Re-ordering the Columns

Now I needed to arrange the columns back into the correct order. (By the way, I should mention, if it is not already obvious, I am presenting these steps in a certain order only for clarity. In reality they were performed haphazardly, and I would often jump back and forth as new ideas came to me.) For this purpose I reached into my now worn "cryptographer's bag of tricks" one last time and utilized something called a "digraphic frequency table". This chart depicts how often, on the average, any two alphabetic letters occur next to each other. For the first two columns in figure x, for example, the combination "YO" occurs only 0.64 times per 1000 letter pairs, "AH" occurs 0.13 times, and so on. By summing up these frequencies for each pair of columns, I was able to calculate which columns were most likely to occur next to each other. The final solution is presented in figures 26 and 27.

```
F L I C K E R B U T P R E S E N T L Y D E T A I
O L E A L I T T L E I I N S E R T E D T H E C A
A S R E M O V E D W I T H T R E M B L I N G H A
S L O W L Y D E S P A R A T L Y S L O W L Y T H

L S O F T H E R O O M W I T H I N E M E R G E D
N D L E A N D P E E R E D I N T H E H O T A I R
N D S I M A D E A T I N Y B R E A C H I N T H E
E R E M A I N S O F P A S S A G E D E B R I S T

F R O M T H E M I S T X C A N Y O U S E E A N Y
E S C A P I N G F R O M T H E C H A M B E R C A
U P P E R L E F T H A N D C O R N E R A N D T H
H A T E N C U M B E R E D T H E L O W E R P A R

T H I N G Q
U S E D T H E F L A M E T O
E N W I D E N I N G T H E
T O F T H E D O O R W A Y W
```

Figure 26. Ordered Columns for Part IV

SLOWLY DESPARATLY SLOWLY THE REMAINS OF
PASSAGE DEBRIS THAT ENCUMBERED THE LOWER
PART OF THE DOORWAY WAS REMOVED WITH
TREMBLING HANDS I MADE A TINY BREACH IN THE
UPPER LEFT HAND CORNER AND THEN WIDENING THE
HOLE A LITTLE I INSERTED THE CANDLE AND
PEERED IN THE HOT AIR ESCAPING FROM THE
CHAMBER CAUSED THE FLAME TO FLICKER BUT
PRESENTLY DETAILS OF THE ROOM WITHIN EMERGED
FROM THE MIST. CAN YOU SEE ANYTHINGQ?

Figure 27. Correctly Ordered Text for Part IV

I have been told by people, although I have not checked it myself, that this is a quote from a Howard Carter book on the opening of King Tut's tomb. Note the troublesome "Q" at the end--I tripped over this more times than I can remember. When I first looked at this part of the code, I thought I could use the "Q" to help me solve the message, since I thought it would absolutely have to be followed by a "U". However, this turned out to be a false lead (one of many).

A New Lead?

Even though it was not necessary to determine the keywords used in the substitution code in order to read Parts I, II and III, I was curious to find out what they were. It was easy enough at this point--just find the plaintext letters in the top row of the Vigenere tableau in figure 1, follow those columns down until the ciphertext letter is found, and then read off the first letters of those rows for the keyword letters. (By the way, because the Kryptos cipher actually uses a modified version of the Vigenere code, the alphabets down the left-hand side and along the top of figure 1 must first be removed for this to work properly.) It turned out that the 8-letter keyword for Part I was "ABSCISSA", and the 10-letter keyword for Parts II and III was "PALIMPSEST". I knew what an "abscissa" was, but this other word was not familiar to me. I looked in up in the dictionary, and found that it was "a written document...that has been written upon several times, often with remnants of earlier...writing still visible." Very interesting. Is the cipher trying to tell us that the Kryptos sculpture contains multiple layers of code--written one on top of the other?

I went back to the I.C. calculations for Part I and found a surprise when they were extended out to 15 alphabets:

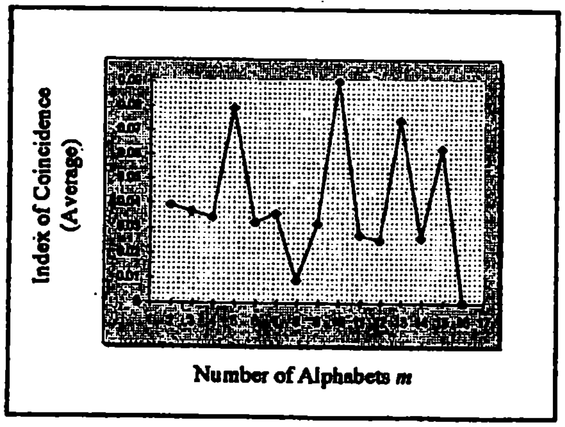


Figure 28. I.C. vs. Number of Alphabets for Part I, Extended To 15 Alphabets

Of course, I knew that the peak at m=10 was caused by the 10-letter keyword, and the peaks at 5 and 15 are expected artifacts of the keyword (1/2 and 2 times the keyword length, respectively). But what was this peak at m=13? Whatever it was, it also showed up in the I.C. plot for Part II (figure 9). Could this be a sign of another code--possibly one using a keyword of 13 letters?

And what about Part V of the puzzle? I haven't spent much time on this portion, but I have already made some headway. There are interesting patterns in here as well, and I see many avenues of assault. Although this part could well be much more difficult than the previous pieces, I am confident that it is not impossible. I doubt that the code's authors would get much pleasure out of writing an unbreakable code.

Final Thoughts

I hope at the very least I have inspired some people to study the Kryptos puzzle and give it a try--there is still much to do. Even the parts of the code that have been decrypted must still be interpreted for their deeper meaning. There are many pieces to be put together, and many layers to be peeled back.

Nothing is more frustrating than reading a cryptography book where the author easily and in a straight-forward manner shows how a code was solved. It's a little like reading one of those books on "How I made a million dollars". The methods typically work for that particular set of circumstances, but they often don't work in your particular case. Similarly, codes have distinct characteristics that frequently require each of them to be solved with a unique method. Since I didn't see any need to dwell on the hundreds of things that I tried that didn't work, the methodologies that I presented may seem a little too straight-forward and deceptively easy.

I genuinely enjoyed working on the Kryptos ciphers. Certainly professional cryptographers could have broken these codes much faster, and would have used superior methods. But I doubt that they would have derived as much satisfaction as I have. I didn't use any computers to decrypt the Kryptos codes--just pencil and paper, some common sense, and a lot of perseverance. I believe that, when confronted with a problem like the Kryptos puzzle, sometimes we need to step back, set aside our computers and preconceived notions and just think. It's important to remember that the Internet, although useful for some applications, doesn't always have the answers; it would have been of little help in solving the Kryptos puzzle.

Maybe it's time to start using our minds again before we automatically reach for our computers.