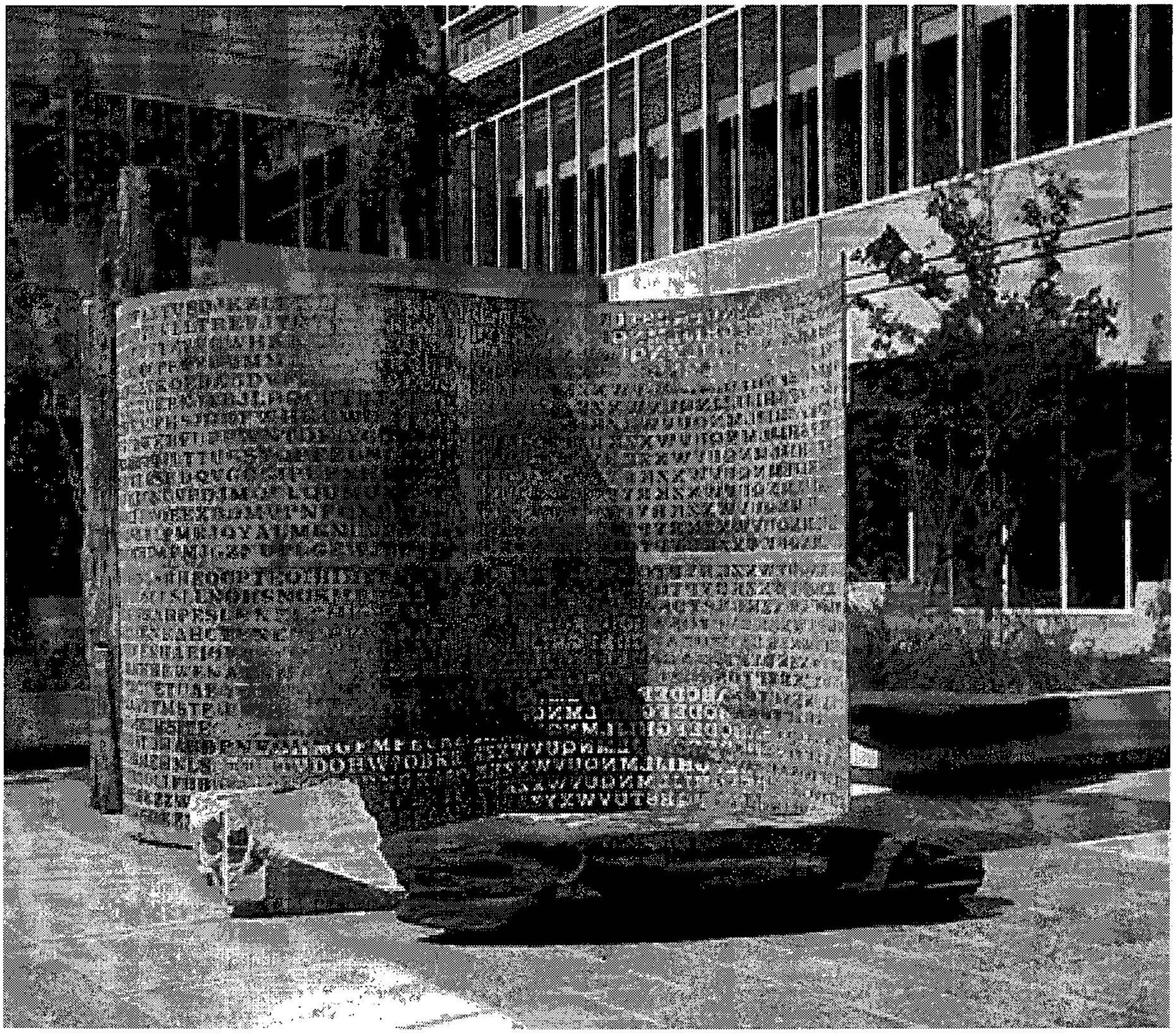
(U) THE CIA KRYPTOS SCULPTURE: A summary of previous work and new revelations in working toward its complete solution

by

[redacted]

PL 86-36/50 USC 3605



(U//~~FOUO~~) Back in 1990, the Central Intelligence Agency's Fine Arts Commission canvassed Washington, DC, area artists, asking for proposals for costs and designs for a sculpture which would be erected in the CIA's new Courtyard outside its cafeteria. The winning sculptor was James Sanborn, and he created a nice little puzzle. It stands about 3 metres (10 feet) tall, and consists of two curved copper plates standing side-by-side, forming an "S" shape if viewed from above.

(U//~~FOUO~~) Before we look at the cipher on the sculpture, here's what James Sanborn had to say about his creation on November 3, 1990, the day it was dedicated:

> "The stonework at the entrance and in the courtyard served two functions. First, it creates a natural framework for the project as a whole, and is part of a landscaping scheme designed to recall the natural stone outcropping that existed on the site before the Agency, and that will endure, as do mountains.
>
> "Second, the tilted strata tell a story like pages of a document. Inserted between these stone pages is a flat copper sheet through which letters and symbols have been cut. This code, which includes certain ancient ciphers, begins as international morse, and increases in complexity as you move through the piece at the entrance and into the courtyard. Its placement in a geologic context reinforces the text's hiddenness as if it were a fossil, frozen in time."

(U//~~FOUO~~) On the left side of the sculpture are letters punched through the copper and reading forward, creating a cipher message. On the right side are letters punched through in reverse and form a "Vigenere Square." On the following page is the Vigenere square which appears in reverse on the right side when looking at the sculpture head-on as it appears in the picture on the first page:

(U//~~FOUO)~~ Fig. 1. Vigenere Square from KRYPTOS sculpture

	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	L
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	
	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	

(U//~~FOUO~~) There are 28 lines on this side of the sculpture. On the top row is the A-Z alphabet, followed immediately by the first four letters of the alphabet, ABCD, making a total of 30 characters on the first line. On each of the next 26 lines, the A-Z alphabet appears in the first position on each of the lines. Following the "A" at the start of the second line, is a keyword-mixed alphabet based on the word "KRYPTOS". After the Z at the end of the 26-long KRYPTOS alphabet, the first four letters of KRYPTOS appear again, to make a total of 31 characters appearing on the line. On the third line, following the "B," appears the same KRYPTOS alphabet, but shifted one spot so that it begins with the letter R. Once the entire shifted 26-long KRYPTOS sequence is used (R through K in this instance), the first four letters of that shifted alphabet then reappear at the end of the line (RYPT in this case).

(U//~~FOUO~~) This process continues through the rest of the 26 lines labeled A-Z at the beginning of each line, except for the line labeled "N." On this line, the shifted KRYPTOS sequence begins GHIJ..., and finishes ...CDEF..., but instead of following with the first four letters from that offset, GHIJ, five letters appear instead, GHIJL.

(U//~~FOUO~~) The 28th line of the Vigenere Square is just a repeat of the top line, the A-Z alphabet followed by the letters ABCD. So we have two things to notice from this side of the sculpture: we have the Direct Standard alphabet (A-Z), and a KRYPTOS keyword-mixed sequence.

(U//~~FOUO~~) Below is a copy of the cipher side of the sculpture:

(U//~~FOUO~~) Fig. 2. Cipher side of sculpture

```
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 E
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 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
```

(U//~~FOUO~~) There are 869 characters appearing on this side of the sculpture. That count includes the four question marks which are scattered throughout.

(U//~~FOUO)~~ There are a few other things to point out here as well. The 15th line of the cipher begins with the letters END, and of the letters YAHR which follow it, the Y, A, and R are raised up about 1 cm. (about 1/2 inch). This made analysts at NSA wonder is the END was perhaps the end of a certain portion of cipher. And maybe the Y, A and R floating in the air a bit higher than the other letters on that line may signify something else as well.

(U//~~FOUO)~~ Well, in February of 1999, a CIA employee named David Stein, stated to the world that he had solved three of four sections of the sculpture. And the world pretty much ignored him. Then just four months later in June 1999, a private citizen in California named James Gillogly, who had a hand in developing the CRYSS software for the FBI, announced on the Internet that he had also solved three of four parts.

(U//~~FOUO)~~ Gillogly received all sorts of accolades for his accomplishments from the media, which made Mr. Stein at the CIA a bit miffed. You see, Mr. Stein had used just a pencil and paper to come up with his solution, but Mr. Gillogly in California had used his computer to arrive at his answer. Mr. Stein believed it to be "cheating" to use a computer, but Mr. Gillogly was quickly supported by others within the intelligence community as anyone working for such an Agency would almost certainly use a computer when solving codes and ciphers.

~~(C//SI)~~ Back in 1992, William Webster, the Director of the CIA at the time, also challenged NSA to read the cipher, and my fellow colleagues also read three of four parts. It's just that it was seven years before these other individuals.

(U//~~FOUO)~~ After the findings presented by Mr. Stein and Mr. Gillogly, [redacted] presented a talk on September 14, 1999, on the work done by NSA seven years prior. The Internet was just beginning to grow at that point in time, and he kept an eye out for someone who might be the first to solve remaining portion of the cipher.

PL 86-36/50 USC 3605

(U//~~FOUO)~~ This was one thing that Lance found:

(U//~~FOUO)~~ Fig. 3. From website claiming to have the solution to the KRYPTOS scuplture.

```
cipher beginning:  E M U F P H Z L R
   repeating key:  K R Y P T O S K R
                   -----------------
           plain:  P E T V J W R W J

Line 1:  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
Line 2:  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
Line 3:  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
Line 4:  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
Line 5:  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
Line 6:  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
Line 7:  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
Line 8:  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
Line 9:  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
```

(U//~~FOUO)~~This particular individual started with the beginning of the cipher itself, EMUFPH-ZLR. He happened to notice the KRYPTOS alphabet in the Vigenere Square, and so he tried a very reasonable thing, simple addition. E is the 5th letter of the alphabet, and K is the 11th letter of the alphabet, so if we add 5 and 11 we get 16, and P is the 16th letter of the alphabet. Then M, the 13th letter, is added to R, the 18th letter. That adds up to 33, but in mod26 arithmetic, that's 5, which is an E. The same process continues until PETVJWRWJ is obtained.

(U//~~FOUO)~~ Now, that's not plaintext, but if you begin with each of those letters, and extend the A-Z alphabet out beyond them, in one of the columns reading down you get GVKMANINA, and JOB at the bottom of the column immediately to its right. According to the web site, GVK-MAN IN A JOB is the solution. His website also highlights the word APE reading down in the first three rows of one of the columns.

(U//~~FOUO)~~ The website explains:

> "The Sanborn sculpture is an homage to CIA agents at work, wherever they may be. For those of you who want to know the rest, it gets somewhat tougher as you move on.
>
> "Good luck! P.S. I am not an agent. I am just ostensibly good at deciphering codes and mysteries."

~~(C//SI)~~ For most people at NSA, most thought there were three sections. The first section contained the first 14 lines, and I'll talk about it in a bit. The next 11 lines were believed to be a transposition as they had a distribution of letters that resembled that of English plaintext. The final three lines were unknown.

(U//~~FOUO)~~We'll examine the top 14 lines first:

(U//~~FOUO)~~ Fig. 4. Top 14 lines of cipher

```
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
```

(b)(1)
(b)(3)-50 USC 3024(i)
PL 86-36/50 USC 3605

[redacted]

(U//~~FOUO~~) The strength in polyalphabetic substitution is that the same plaintext letter will not always be enciphered to the came cipher letter as each encipherment is dependent upon the alphabet enciphering it. And with multiple alphabets, there are multiple ways for each plaintext value to change. Similarly, identical ciphertext letters did not always evolve from the same plaintext value: they can be spawned from two entirely different plaintext values.

(U//~~FOUO~~) The weakness of polyalphabetic substitution is if you have a rather long message, then the frequency counts of each of the alphabets will begin to look like some offset of some alphabet. Luckily for us we have 432 characters and eight alphabets, so that should be long enough for us to make some headway in solving.

(U//~~FOUO~~) Given that the sculpture mentions the `A-Z` alphabet, as well as the `KRYPTOS` keyword-mixed alphabet, these two alphabets seemed to be the reasonable places to begin. It may very well be something different, but it pays to try the easiest thing first, and if that doesn't produce results, advance to something else.

(U//~~FOUO~~) Fig. 6. Alphabet frequencies for eight alphabets, Direct Standard order

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
-	-	4	2	2	2	2	2	2	1	1	1	-	8	2	3	2	8	2	-	1	1	3	-	1	4
2	1	-	3	5	4	3	4	-	5	1	4	2	-	-	2	3	3	1	1	3	1	3	-	1	2
3	-	-	3	1	-	7	3	1	3	2	1	1	2	-	-	10	2	1	3	1	3	1	1	4	1
1	3	-	3	1	2	-	-	1	2	7	4	-	4	-	5	2	-	-	4	7	2	-	2	1	3
3	1	1	11	3	7	2	-	2	2	-	2	3	1	-	3	3	-	1	-	3	1	-	1	2	2
1	-	-	4	7	9	1	1	1	1	1	6	2	-	-	-	4	1	-	1	4	-	1	3	1	5
-	2	-	1	6	4	2	3	1	-	-	3	6	1	-	1	1	1	1	5	2	9	-	2	-	3
-	1	2	1	6	3	7	3	-	2	6	1	5	1	1	2	4	-	-	2	3	3	-	-	1	-

(U//~~FOUO~~) Fig. 7. Alphabet frequencies for eight alphabets, KRYPTOS keyword-mixed order

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
1	8	1	3	-	2	2	-	-	4	2	2	2	2	2	2	1	1	-	8	2	1	1	3	-	4
1	3	1	2	1	-	1	2	1	-	3	5	4	3	4	-	5	4	2	-	3	3	1	3	-	2
2	2	4	-	3	-	1	3	-	-	3	1	-	7	3	1	3	1	1	2	10	1	3	1	1	1
7	-	1	5	4	-	-	1	3	-	3	1	2	-	-	1	2	4	-	4	2	7	2	-	2	3
-	-	2	3	-	-	1	3	1	1	11	3	7	2	-	2	2	2	3	1	3	3	1	-	1	2
1	1	1	-	1	-	1	1	-	-	4	7	9	1	1	1	1	6	2	-	4	4	-	1	3	5
-	1	-	1	5	-	1	-	2	-	1	6	4	2	3	1	-	3	6	1	1	2	9	-	2	3
6	-	1	2	2	1	-	-	1	2	1	6	3	7	3	-	2	1	5	1	4	3	3	-	-	-

(U//~~FOUO)~~Looking at these frequency distributions, someone noticed that the sixth line of the KRYPTOS alphabet frequencies looked good when the alphabet was slid at this offset:

(U//~~FOUO)~~Fig. 8. Sixth KRYPTOS alphabet frequencies slid against KRYPTOS sequence.

1	1	1	-	1	-	1	1	-	-	4	7	9	1	1	1	1	6	2	-	4	4	-	1	3	5
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

(U//~~FOUO)~~ And looking at the eighth KRYPTOS alphabet frequencies, they looked good when the KRYPTOS alphabet was slid thusly:

(U//~~FOUO)~~Fig. 9. Eighth KRYPTOS alphabet frequencies slid against KRYPTOS sequence.

6	-	1	2	2	1	-	-	1	2	1	6	3	7	3	-	2	1	5	1	4	3	3	-	-	-
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

(U//~~FOUO~~) These two alphabets matched decently, so they were filled in, and this was the resulting plaintext:

(U//~~FOUO)~~Fig. 10. Plaintext recoveries for sixth and eighth alphabets.

```
EMUFPHZL RFAXYUSD JKZLDKRN SHGNFIVJ YQTQUXQB QVYUVLLT REVJYQTM
     Q X      R L      S K      U W      T I      W E      K Z

KYRDMFDV FPJUDEEH ZWETZYVG WHKKQETG FQJNCEGG WHKK?DQMC PFQZDQMM
     M I      O A      V S      O S      O S      ? H Y      H E

IAGPFXHQ RLGTIMVM ZJANQLVK QEDAGDVF RPJUNGEU NAQZGZLE CGYUXUEE
     M G      F E      E N      T O      A H      N T      I T

NJTBJLBQ CRTBJDFH RRYIZETK ZEMVDUFK SJHKFWHK UWQLSZFT IHHDDDUV
     E G      T A      O N      I N      L N      N W      T I

H?DWKBFUF PWNTDFIY CUQZEREE VLDKFEZM OQQJLTTU GSYQPFEU NLAVIDXF
 ?    S O      S U      U T      O E      X H      S H      T O

LGGTEZ?FK ZBSFDQVG OGIPUFXH HDRKFFHQ NTGPUAEC NUVPDJMQ CLQUMUNE
     N? N      H S      S A      S G      R Y      D G      I T

DFQELZZV RRGKFFVO EEXBDMVP NFQXEZLG REDNQFMP NZGLFLPM RJQYALMG
     N I      S X      F V      N S      S V      E E      E S

NUVPDXVK PDQUMEBE DMHDAFMJ GZNUPLGE WJLLAETG
     M N      O T      S C      E T      O S
```

(U//~~FOUO)~~One thing that needs to be pointed out: the question marks were ignored in the counting of the alphabets. This work seems to have gone well. There are a limited number of letters that can be placed between the recoveries made to this point.

(U//~~FOUO~~) Continuing work in this fashion, if one guessed an "I" occurs between the "S" and "X" on the next to last line, the resulting recoveries look like this:

(U//~~FOUO~~) Fig. 11. Plaintext recoveries for sixth, seventh and eighth alphabets.

```
EMUFPHZL RFAXYUSD JKZLDKRN SHGNFIVJ YQTQUXQB QVYUVLLT REVJYQTM
     QSX      RGL      SBK      UPW      TRI      WXE      KEZ

KYRDMFDV FPJUDEEH ZWETZYVG WHKKQETG FQJNCEGG WHKK?DQMC PFQZDQMM
     MLI      OTA      VIS      OWS      OSS     ? HEY      HEE

IAGPFXHQ RLGTIMVM ZJANQLVK QEDAGDVF RPJUNGEU NAQZGZLE CGYUXUEE
     MAG      FIE      EIN      TIO      ATH      NDT      ITT

NJTBJLBQ CRTBJDFH RRYIZETK ZEMVDUFK SJHKFWHK UWQLSZFT IHHDDDUV
     ERG      TOA      OWN      ION      LAN      NOW      THI

H?DWKBFUF PWNTDFIY CUQZEREE VLDKFEZM OQQJLTTU GSYQPFEU NLAVIDXF
 ?    SHO      SBU      UTT      OME      XWH      STH      TLO

LGGTEZ?FK ZBSFDQVG OGIPUFXH HDRKFFHQ NTGPUAEC NUVPDJMQ CLQUMUNE
     N?ON      HIS      SLA      SAG      RTY      DEG      IFT

DFQELZZV RRGKFFVO EEXBDMVP NFQXEZLG REDNQFMP NZGLFLPM RJQYALMG
     NMI      SIX      FIV      NDS      SEV      EVE      EES

NUVPDXVK PDQUMEBE DMHDAFMJ GZNUPLGE WJLLAETG
     MIN      ORT      SEC      EST      OWS
```

(U//~~FOUO~~) Work continued in this mode, adding on a letter to either end of the recoveries made to this point. Staying with the next to last line, it appears numbers were being spelled out. SIX already appeared, and it also looks as if FIVE, SEVEN, and THREE occur later on that line.

(U//~~FOUO~~) The only portion of the message where things don't look good is at the top. The recoveries there are ugly! QSX. SBK. WXE. All nasty-looking trigraphs in English. But things look pretty good from the second line forward.

(U//~~FOUO~~) Continuing to expand these trigraphs into longer stretches of plaintext, we eventually get this:

(U//~~FOUO~~) Fig. 12. Plaintext recoveries for top 14 lines of KRYPTOS sculpture.

```
EMUFPHZL RFAXYUSD JKZLDKRN SHGNFIVJ YQTQUXQB QVYUVLLT REVJYQTM
NXTRCQSX CMJGBRGL XSBSJSBK HQVBMUPW DKGCRTRI YYEDYWXE CLOOBKEZ

KYRDMFDV FPJUDEEH ZWETZYVG WHKKQETG FQJNCEGG WHKK?DQMC PFQZDQMM
BBDZXMLI TWASTOTA LLYINVIS IBLEHOWS THATPOSS IBLE?THEY USEDTHEE

IAGPFXHQ RLGTIMVM ZJANQLVK QEDAGDVF RPJUNGEU NAQZGZLE CGYUXUEE
ARTHSMAG NETICFIE LDXTHEIN FORMATIO NWASGATH EREDANDT RANSMITT

NJTBJLBQ CRTBJDFH RRYIZETK ZEMVDUFK SJHKFWHK UWQLSZFT IHHDDDUV
EDUNDERG RUUNDTOA NUNKNOWN LOCATION XDOESLAN GLEYKNOW ABOUTTHI

H?DWKBFUF PWNTDFIY CUQZEREE VLDKFEZM OQQJLTTU GSYQPFEU NLAVIDXF
S?THEYSHO ULDITSBU RIEDOUTT HERESOME WHEREXWH OKNOWSTH EEXACTLO

LGGTEZ?FK ZBSFDQVG OGIPUFXH HDRKFFHQ NTGPUAEC NUVPDJMQ CLQUMUNE
CATION?ON LYWWTHIS WASHISLA STMESSAG EXTHIRTY EIGHTDEG REESFIFT

DFQELZZV RRGKFFVO EEXBDMVP NFQXEZLG REDNQFMP NZGLFLPM RJQYALMG
YSEVENMI NUTESSIX POINTFIV ESECONDS NORTHSEV ENTYSEVE NDEGREES

NUVPDXVK PDQUMEBE DMHDAFMJ GZNUPLGE WJLLAETG
EIGHTMIN UTESFORT YFOURSEC ONDSWEST IDBYROWS
```

(U//~~FOUO~~) The plaintext reads:

> "IT WAS TOTALLY INVISIBLE HOW IS THAT POSSIBLE ? THEY USED
> THE EARTH'S MAGNETIC FIELD X THE INFORMATION WAS GATHERED
> AND TRANSMITTED UNDERGRUUND TO AN UNKNOWN LOCATION X
> DOES LANGLEY KNOW ABOUT THIS ? THEY SHOULD IT'S BURIED
> OUT THERE SOMEWHERE X WHO KNOWS THE EXACT LOCATION ?
> ONLY W W THIS WAS HIS LAST MESSAGE X THIRTY-EIGHT DEGREES
> FIFTY-SEVEN MINUTES SIX POINT FIVE SECONDS NORTH SEVENT-
> SEVEN DEGREES EIGHT MINUTES FORTY-FOUR SECONDS WEST I D
> BY ROWS

(U//~~FOUO~~) It should be pointed out that UNDERGRUUND is a misspelling of "UNDERGROUND," but that's exactly how it decrypts.

(U//~~FOUO~~) As to the information transmitted underground, and exactly what's buried out there, your guess is as good as mine. However, the WW almost certainly refers to William Webster who was director of the CIA when the sculpture was commissioned.

(U//~~FOUO~~) The meaning of the last portion, I D BY ROWS, was a stumper, and we'll return to this later to see what it really means.

(U//~~FOUO~~) If you follow through to obtain the matrix used to encipher this portion of the sculpture, this is the periodic polyalphabetic matrix obtained:

(U//~~FOUO~~) Fig. 13. Enciphering matrix for portion of KRYPOS Sculpture

P:	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
C1:	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
C2:	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
C3:	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
C4:	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
C5:	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
C6:	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
C7:	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
C8:	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

(U//~~FOUO~~) The plain and cipher components both use the keyword-mixed sequence based on KRYPTOS, with the cipher offset according to the repeating key of ABSCISSA, which can be seen reading down the column beneath the plaintext letter A. To refresh your memory, an abscissa is the horizontal cartesian coordinate on a plane measured from the y-axis along the line parallel to the x-axis at point p. How this fits in to the overall solution of the sculpture remains to be seen.

(U//~~FOUO~~) Originally we believed there were three portions to the cipher. Suddenly, the first part has become two parts, and we've read just one part of what is now a four-part puzzle.

(U//~~FOUO~~) Next, let's look at the section that contains lines 15-25 of the cipher. This section was believed to be enciphered by a transposition.

(b)(1)
(b)(3)-50 USC 3024(i)
PL 86-36/50 USC 3605

(U//~~FOUO~~) Fig. 14. Lines 15-25 of the KRYPTOS sculpture

```
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 E
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 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//~~FOUO~~) The approach tried by those working on the cipher was a reasonable one for those attempting to solve a transposed message. It was noticed that there was exactly one Q appearing in this section of the cipher. A letter U would probably follow it, and there were five Us appearing in this portion of the cipher. So a reasonable thing to do when attempting to determine the transposition matrix used is take the stretch of cipher containing the Q, and take a handful of letters before and after it, and write them as a column. Then take all the occurrences of U, and also grab a couple letters before and after them, writing them in as a column immediately to the right of the column with the Q.

(U//~~FOUO~~) Fig. 16. Lines 15-25 with stretches of cipher containing the Q and the Us aligned columnarly. Extracted stretches are underlined to assist the reader in finding their location within the cipher. Stretches containing U are underlined once. The stretch with the Q is doubly underlined.

```
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 E
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 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


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

(U//~~FOUO~~) The idea is to find columns that look like portions of readable English text. None of these looks too bad. Any of them could contain short stretches of English. The YY in the first column might be a little problematic, as is the HH (unless the plaintext is talking about Fishhooks or something). The third alignment here looks pretty good. The EO could occur in the word PEOPLE, or THE ONLY if it was two words. Beneath the QU we have HE which looks really good for THE. So it was decided to try to build upon that.

(U//~~FOUO~~) Another stretch of cipher that looked good when placed to the left of the QU was found.

(U//~~FOUO~~) Fig. 17. Three stretches of Lines 15-25 aligned columnarly.

```
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 E
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 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

                          L Y F
                          E T I
                          H E O
                          A Y T
                          G Q U
                          T H E
                          D E T
                          H E U
                          A N A
```

(U//~~FOUO~~) Again, things look nice. Before the QU is a word ending with G. The AYT above it could be from DAY TIME or something like that. HEO above it could be THE ONLY. ETI above it could be SAME TIME, or something along those lines. More progress was made as additional cipher stretches were extracted and added to the left of these three columns.

(U//~~FOUO)~~ Fig. 18. Five stretches of cipher from Lines 15-25 extracted and aligned columnarly

```
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 E
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 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

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

(U//~~FOUO~~) Still looks good! A word ending with ING precedes the QU. Above the QU it looks like UNDERWAY or STAIRWAY followed by a word starting with T.

(U//~~FOUO~~) Work continued in this fashion until finally, the plaintext and its matrix were found! An incompletely filled transposition matrix with four rows and 86 columns was recovered. Here's the matrix which was used, split in two so it would fit below:

(U//~~FOUO~~) Fig. 19. Incompletely filled 4x86 transposition matrix used to encipher lines 15-25.

```
1    SLOWLYDESPARATLYSLOWLYTHEREMAINSOFPASSAGEDE...
2    ASREMOVEDWITHTREMBLINGHANDSIMADEATINYBREACH...
3    OLEALITTLEIINSERTEDTHECANDLEANDPEEREDINTHEH...
4    FLICKERBUTPRESENTLYDETAILSOFTHEROOMWITHINEM...


        ...BRISTHATENCUMBEREDTHELOWERPARTOFTHEDOORWAYW    1
        ...INTHEUPPERLEFTHANDCORNERANDTHENWIDENINGTHEH    2
        ...OTAIRESCAPINGFROMTHECHAMBERCAUSEDTHEFLAMETO    3
        ...ERGEDFROMTHEMISTXCANYOUSEEANYTHINGQ            4
```

(U//~~FOUO)~~The plaintext from this portion of the cipher reads:

> "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 X CAN YOU SEE ANYTHING Q"

(U//~~FOUO~~) This passage is from a book written by Howard Carter, and it's referring to the opening of King Tut's tomb back in November 1922.

(U//~~FOUO)~~ A couple of other things also need to be pointed out. There's another misspelling. The second word of the decrypting of this passage, DESPARATLY should be DESPERATELY, but it did indeed decrypt as shown above. Also, remember how the solution to this portion of the cipher began by placing a U next to the Q? Well, in the solution the Q is not followed by a U. Good luck never hurts when doing cryptanalysis.

(U//~~FOUO)~~ Working back to discover the order in which the columns were extracted from this transposition matrix, we recall that the cipher began with END, followed by the YAHR in which the Y, A and R were slightly raised on the sculpture. The END occurs near the right side of the matrix, and reads from bottom to top. YAHR was the second column extracted from the matrix. It's seven columns to the left of the END column, and also was extracted from bottom to top. Seven more columns to the left we see OHNL reading upwards. In fact, this "seven columns to the left" property continues throughout the entire process.

(U//~~FOUO)~~Fig. 20. Enumeration of the columns by the order in which they were extracted

```
1   SLOWLYDESPARATLYSLOWLYTHEREMAINSOFPASSAGEDE...
2   ASREMOVEDWITHTREMBLINGHANDSIMADEATINYBREACH...
3   OLEALITTLEIINSERTEDTHECANDLEANDPEEREDINTHEH...
4   FLICKERBUTPRESENTLYDETAILSOFTHEROOMWITHINEM...
                                9     8     7

          ...BRISTHATENCUMBEREDTHELOWERPARTOFTHEDOORWAYW   1
          ...INTHEUPPERLEFTHANDCORNERANDTHENWIDENINGTHEH   2
          ...OTAIRESCAPINGFROMTHECHAMBERCAUSEDTHEFLAMETO   3
          ...ERGEDFROMTHEMISTXCANYOUSEEANYTHINGQ           4
             6     5     4     3     2     1
```

(U/~~/FOUO)~~ Because of the values are occurring at an interval of seven, we can actually recreate a matrix that's seven columns wide to represent the ordering of the columns. The number 49 represents the leftmost column, FAOS when reading from bottom to top. It was the 49th column extracted from this matrix. Next, the 12 represents the second column from the left, LLSL when reading upward. It was the 12th column pulled from the matrix.

(U/~~/FOUO)~~Fig. 21. Matrix containing the order in which the columns were extracted, reading left to right, top to bottom.

49	12	61	24	73	36	85
48	11	60	23	72	35	84
47	10	59	22	71	34	83
46	9	58	21	70	33	82
45	8	57	20	69	32	81
44	7	56	19	68	31	80
43	6	55	18	67	30	79
42	5	54	17	66	29	78
41	4	53	16	65	28	77
40	3	52	15	64	27	76
39	2	51	14	63	26	75
38	1	50	13	62	25	74
37	86					

(U/~~/FOUO)~~Within this box there is a nice ordering. 1-12 in the second column, 13-24 in the 4th column, 25-36 in the sixth column, 37-49 in the first column, 50-61 in the third column, 62-73 in the fifth column, 74-85 in the seventh column, and at the very bottom of the second column is the 86.

(U//~~FOUO~~) It was noticed that if these columns are ordered, they form a numeric key of 4 1 5 2 6 3 7. If a numeric key is created form the word KRYPTOS, it would be 1 4 7 3 6 2 5. If this order is written in reverse beginning with the R column, the one labeled with a 4, we would get the 4 1 5 2 6 3 7 order..

(U//~~FOUO~~) Fig. 22. An attempt to explain the ordering of the column key values

R	K	S	O	T	P	Y
4	1	5	2	6	3	7
49	12	61	24	73	36	85
48	11	60	23	72	35	84
47	10	59	22	71	34	83
46	9	58	21	70	33	82
45	8	57	20	69	32	81
44	7	56	19	68	31	80
43	6	55	18	67	30	79
42	5	54	17	66	29	78
41	4	53	16	65	28	77
40	3	52	15	64	27	76
39	2	51	14	63	26	75
38	1	50	13	62	25	74
37	86					

(b)(1)
(b)(3)-50 USC 3024(i)
PL 86-36/50 USC 3605

(U//~~FOUO~~) At this point, having solved two of three parts, work returned to the first two lines of cipher on the sculpture, which consisted of 63 characters.

(U//~~FOUO~~) Fig. 23. First two lines of KRYPTOS sculpture

```
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
```

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
PL 86-36/50 USC 3605

[redacted]

(U//~~FOUO)~~Because it worked so well the last time, frequency counts were made for five alphabets with the cipher arranged in KRYPTOS keyword-mixed order.

(U//~~FOUO)~~Fig. 25. Frequency counts using 5 alphabets for the first 63 characters of cipher.

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
-	-	-	-	-	-	-	1	-	-	2	1	-	-	2	-	-	1	2	-	2	-	2	-	-	-
2	-	-	-	-	-	-	-	-	-	-	-	1	1	-	-	3	1	1	-	-	1	1	-	1	1
1	1	5	-	1	-	-	-	-	-	1	-	-	-	-	-	-	1	-	1	-	1	-	-	1	-
-	3	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	1	3	2	-	-	-	1
-	-	-	1	2	-	2	-	1	-	1	1	1	-	-	1	-	1	-	-	-	-	1	-	-	-

(U//~~FOUO)~~Five occurrences of the cipher letter Y in the third alphabet were immediately noticed. The easiest thing to try is to match the most frequently occurring character in English, E, to the cipher Y and see what happens. Using the KRYPTOS keyword-mixed alphabet again, just because it worked so well last time, we get this alignment and plaintext:

(U//~~FOUO)~~Fig. 26. Alignment of KRYPTOS keyword-mixed alphabet with frequencies from third cipher alphabet, and resulting plaintext:

```
1 1 5 - 1 - - - - - 1 - - - - - - 1 - 1 - 1 - - 1 -
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

EMUFP HZLRF AXYUS DJKZL DKRNS HGNFI VJYQT QUXQB
..T.. ..K.. ..E.. ..C.. ..D.. ..Y.. ..E.. ..A..

QVYUV LLTRE VJYQT MKYRD MFD
..E.. ..G.. ..E.. ..E.. ..N
```

(U//~~FOUO~~) Nothing looks terrible here, but there's nothing really to build off, like a Q to place a U after. Eventually, it was discovered that the first alphabet frequencies matched pretty well with this alignment, giving these recoveries:

(U//~~FOUO)~~Fig. 27. Alignment of KRYPTOS keyword-mixed alphabet with frequencies from first cipher alphabet, and resulting plaintext

```
- - - - - - - 1 - - 2 1 - - 2 - - 1 2 - 2 - 2 - - -
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

EMUFP HZLRF AXYUS DJKZL DKRNS HGNFI VJYQT QUXQB
B.T.. E.K.. T.E.. A.C.. A.D.. E.Y.. N.E.. L.A..

QVYUV LLTRE VJYQT MKYRD MFD
L.E.. H.G.. N.E.. I.E.. I.N
```

(U//~~FOUO)~~This looks very good as there are a limited number of recoveries that can be placed between some of these recoveries. Certainly a vowel needs to land between the B and T at the beginning in the second alphabet. And at the very end, maybe an O between the I and N. That was attempted, and this is what happened:

(U//~~FOUO)~~ Fig. 28. Alignment of KRYPTOS keyword-mixed alphabet with frequencies from second cipher alphabet, and resulting plaintext:

```
2 - - - - - - - - - - - 1 1 - - 3 1 1 - - 1 1 - 1 1
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

EMUFP HZLRF AXYUS DJKZL DKRNS HGNFI VJYQT QUXQB
BET.. EMK.. TLE.. ACC.. AND.. ESY.. NCE.. LHA..

QVYUV LLTRE VJYQT MKYRD MFD
LIE.. HDG.. NCE.. INE.. ION
```

(U//~~FOUO)~~ We didn't do too badly. While we may have hoped for an H to land between the T and E, we got TLE. But that's possible in a word like GENTLE or KETTLE. The ION at the end looks great and we'd like to see a T or S land before it. And the two occurrences of NCE, in words like GLANCE and ONCE look super.

(U//~~FOUO)~~ But there are some recoveries that don't look too great. EMK in the first line is not the nicest letter combination, and the HDG in the bottom line is downright ugly. But then someone thought that the first set of three recoveries (BET) looks good, the second (EMK) doesn't, the third (TLE) looks good, the fourth (ACC) is not so good, the fifth (AND) is good, and so on. It seems to alternate between good and not-so-good all the way through. So maybe it really was periodic polyalphabetic with 10 alphabets.

(U//~~FOUO)~~ If the assumption that 10 alphabets and polyalphabetic substitution is used, this is what we have at this point:

(U//~~FOUO)~~Fig. 29. Recoveries for first three alphabets of 10-alphabet polyalphabetic substitution.

```
EMUFPHZLRF AXYUSDJKZL DKRNSHGNFI VJYQTQUXQB
BET....... TLE....... AND....... NCE.......

QVYUVLLTRE VJYQTMKYRD MFD
LIE....... NCE....... ION
```

(U//~~FOUO)~~One nice thing that happens here is that the letter occurring before each of the NCEs is different. They're both most likely vowels. The TLE will serves as a nice confirmation to show this is the right track.

(U//~~FOUO~~) This was done, and here's the resulting plaintext after all the letters were recovered.

(U//~~FOUO~~) Fig. 30. Plaintext for first two lines of KRYPTOS sculpture.

```
EMUFPHZLRF AXYUSDJKZL DKRNSHGNFI VJYQTQUXQB
BETWEENSUB TLESHADING ANDTHEABSE NCEOFLIGHT

QVYUVLLTRE VJYQTMKYRD MFD
LIESTHENUA NCEOFIQLUS ION
```

(U//~~FOUO~~) In a more readable form, the plaintext says:

> "BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF IQLUSION"

(U//~~FOUO~~) Yet another typographical error in the plaintext. The correct decryption is indeed IQLUSION instead of ILLUSION, which is what is obviously meant.

(U//~~FOUO~~) Recovering the polyalphabetic substitution matrix used, the plain and cipher components are the keyword-mixed sequence based on KRYPTOS, with a repeating key of PALIMPSEST.

(U//~~FOUO~~) Fig. 31. Decryption matrix for first two lines of KRYPTOS sculpture.

P:	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
C1:	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
C2:	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
C3:	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
C4:	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
C5:	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
C6:	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
C7:	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
C8:	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
C9:	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
C10:	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

(U//~~FOUO~~) Palimpsest is a noun which means a "parchment, tablet, etc., that has been written upon two or three times, the previous text or texts having been imperfectly erased, and remaining therefore still partly visible."

(U//~~FOUO~~) Between the definition of Palimpsest and the plaintext resulting from this passage, it makes one wonder if there isn't something else on the sculpture that may have been overlooked.

(U//~~FOUO~~) At this point, three of four sections had been decrypted, and for those of us at NSA who've worked on this, and that numbers in the dozens, no one has ever gotten that last part.

(U//~~FOUO~~)However, on April 19, 2006, the sculptor, James Sanborn, admitted publicly that there was an omitted letter in the second portion of the cipher, the section with the latitude and longitude coordinates. Returning to that section, this was the polyalphabetic section with eight alphabets using the repeating key of ABSCISSA.

(U//~~FOUO~~) Fig. 32. Decryption matrix for second portion of KRYPTOS cipher.

P:	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
C1:	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
C2:	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
C3:	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
C4:	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
C5:	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
C6:	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
C7:	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
C8:	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

(U//~~FOUO~~) Recall that the section in question is the one that ends with the "I D BY ROWS"

(U//~~FOUO~~) Fig. 33. End of decryption of second part.

```
...GNUVPDXV KPDQUMEB EDMHDAFM JGZNUPLG EWJLLAET G
...SEIGHTMI NUTESFOR TYFOURSE CONDSWES TIDBYROW S
```

(U//~~FOUO~~) Mr. Sanborn's admission of an omitted letter came after seven years of hearing the phrase "I D BY ROWS," and assuming all along it was some sort of "cryppie talk" used by solvers to explain what they had dome to reach this point. He never intended the cipher to say that, figuring by omitting a letter, it would merely cause the cipher to decrypt to random letters and not really say anything with meaning. And Mr. Sanborn claims that the omitted letter was for "aesthetic reasons," refusing to claim any oversight.

(U//~~FOUO~~) The missing letter was a missing cipher letter S which should occur between the E and the W near the end of the cipher passage. By placing the missing S in its proper place, the new resulting plaintext looks like this:

(U//~~FOUO~~) Fig. 34. Corrected decryption of second part after including missing cipher S.

```
...GNUVPDXV KPDQUMEB EDMHDAFM JGZNUPLG ESWJLLAE TG
...SEIGHTMI NUTESFOR TYFOURSE CONDSWES TXLAYERT WO
```

(U//~~FOUO~~) Instead of ending with "ID BY ROWS", "LAYER TWO" is the new conclusion to this section.

(b)(1)
(b)(3)-50 USC 3024(i)
PL 86-36/50 USC 3605

(U//~~FOUO~~) So this is where we stand today. There are several clues which may or may not pertain to the solution of the missing fourth part. First, the three misspelled words, one from each section: IQLUSION, UNDERGRUUND and DESPARATLY. One person, on their website, tries to be helpful by pointing out that if you take the two words used as repeating keys, ABSCISSSA and PALIMPSEST, you can anagram them to say "P.S. It's as simple as ABC." While that's nice to know, I don't know how it would figure into the actual solution of the fourth part. And we had a missing letter in the second part of the cipher. Could there possibly be a missing letter in the remaining section which is presently making it impossible to find a solution?

(U//~~FOUO~~) Looking at the remaining 97 characters, they have a fairly flat distribution, although there are eight Ks which appear.

[redacted]

(U//~~FOUO)~~ There are no long repeats, but there is a slight interval 7 property.

[redacted]

(U//~~FOUO)~~ I have tried a number of things which might cause an interval 7 property to appear, including Plaintext Autokey and Ciphertext Autokey, but I've yet to stumble upon something that gives either readable plaintext, or hints at the presence of a second encipherment layer.

(U//~~FOUO)~~ Work continues in spits and spurts, depending upon time, motivation, and ideas.

(b)(1)
(b)(3)-50 USC 3024(i)
PL 86-36/50 USC 3605