

memorandum

DATE: 9 June 1993

Z-043-93

REPLY TO
ATTN OF: Z

*PLS FORWARD TO ADMIRAL
STUDEMAN FOR INFO.*

SUBJECT: CIA KRYPTOS Sculpture - Challenge and Resolution ~~(FOUO)~~ -
INFORMATION MEMORANDUM

TO: DIR *M*
THRU: D/DIR *NY*, EXEC/DIR *SD*, DDO *AM* *Great story!*

1. ~~(FOUO)~~ The KRYPTOS sculpture, located at the entrance and in the courtyard of the new CIA headquarters, consists of a series of stone "pages" containing code which begins as International Morse and increases in complexity as the stonework extends into the courtyard. Inserted between these stone "pages" is a flat copper sheet engraved with letters and symbols - the enciphered message - that is the focus of this challenge.

2. ~~(FOUO)~~ In November, a cadre of cryptanalysts assigned to Z Group enthusiastically responded to the challenge. Within one month, three of the four cipher systems used to encrypt the sculpture's plain text had been diagnosed and completely exploited. The cryptographies employed for the encryption of these three parts involved two periodic polyalphabetic substitution ciphers and a keyed columnar transposition cipher. The exploitation of the sculpture's first three parts constitutes a readability of approximately 89%. The final 97 characters continue to elude solution.

3. ~~(FOUO)~~ Attached, for your review, is a brief description of the employed cryptographies and the plain text derived from the three exploited portions of the KRYPTOS sculpture. If your schedule permits, we would be happy to present a 15-minute briefing on the KRYPTOS sculpture solution and introduce you to the cryptanalysts responsible for the success against this cipher.



(b)(3)-P.L. 86-36

3 Encls:

- 1. Copy of Sculpture Picture
- 2. Copy of Cipher
- 3. Description of Cryptographies

cc: Z4
Z43

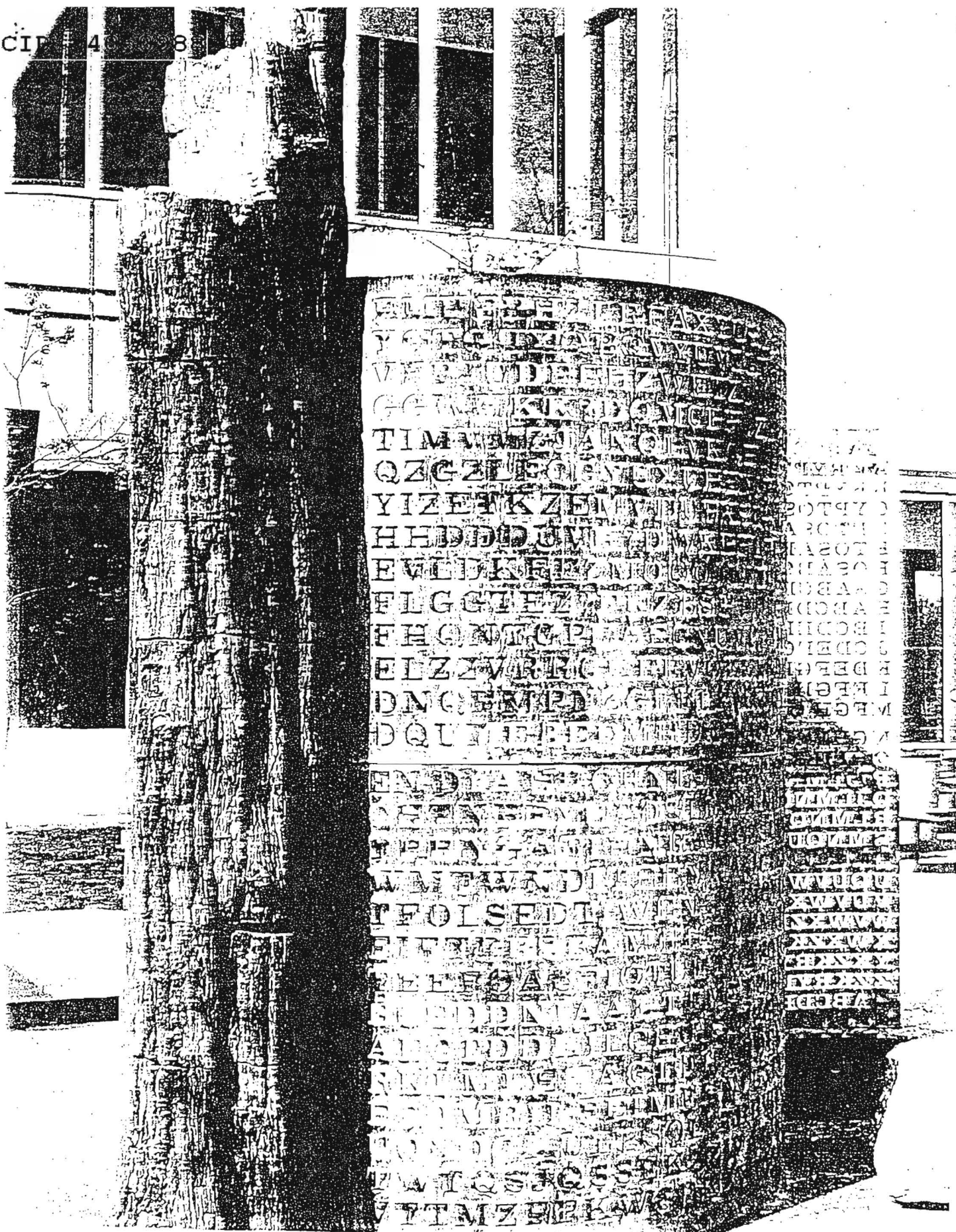
Derived from: NSA Class. Guide 342-97
29 May 1997
Dissem. on: X1, X5

~~SECRET SPOKE~~
~~FOR OFFICIAL USE ONLY~~

OPTIONAL FORM #46695 *



Home Ex Rec 11 June 93



(U)

THE KRYPTOS SCULPTURE CIPHER

~~(b)~~

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 J 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 H 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

PART 1

~~(S)~~

Cryptography: Periodic Polyalphabetic Substitution employing
10 alphabets

Plain component: Keyword mixed sequence based on **KRYPTOS**

Cipher component: Keyword mixed sequence based on **KRYPTOS**

Repeating Key: **PALIMPSEST**

Index letter: **K**

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

EMUFPHZLRF AXYUSDJKZL DKRNSHGNFI VJYQTQUXQB
BETWEENSUB TLESHADING ANDTHABSCE NCEOFLIGHT

QVYUVLLTRE VJYQTMKYRD MFD
LIESTHENUA NCEOFIQLUS ION

(FOUO) Respaced and punctuated, it reads:

"BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF
ILLUSION"

PART 2

~~SECRET~~

Cryptography: Periodic Polyalphabetic Substitution employing
8 alphabets

Plain component: Keyword mixed sequence based on **KRYPTOS**

Cipher component: Keyword mixed sequence based on **KRYPTOS**

Repeating Key: **ABSCISSA**

Index letter: **K**

P: KRYPTOSABCDEFGHIJLMNQUVWXZ
 C1: ABCDEFGHIJLMNQUVWXZKRYPTOS
 C2: BCDEF~~G~~H IJLMNQUVWXZKRYPTOSA
 C3: ~~S~~ABCDEFGHIJLMNQUVWXZKRY~~P~~TO
 C4: ~~C~~DEFGHI~~J~~LMNQUVWXZKRYPTOSAB
 C5: ~~I~~JLMNQ~~U~~VWXZKRYPTOSABCDEFGHI
 C6: ~~S~~ABCDEF~~G~~H IJLMNQUVWXZKRYPTO
 C7: ~~S~~ABCDEF~~G~~H IJLMNQUVWXZKRYPTO
 C8: ~~A~~BCDEF~~G~~H IJLMNQUVWXZKRYPTOS

VFPJUDEE	HZWETZYV	GWHKKQET	GFQJNCEG	GWHKK?DQM
ITWASTOT	ALLYINVI	SIBLEHOW	STHATPOS	SIBLE?THE
CPFQZDQM	MIAGPFXH	QRLGTIMV	MZJANQLV	KQEDAGDV
YUSEDTHE	EARTHSMA	GNETICFI	ELDXTHEI	NEFORMATI
FRPJUNGE	UNAQZGZL	ECGYUXUE	ENJTBJLB	QCETBJDF
ONWASGAT	HEREDAND	TRANSMIT	TEDUNDER	GROUNDTO
HRRYZET	KZEMVDUF	KSJHKFWH	KUWQLSZF	TIHHDDDU
ANUNKNOW	NLOCATIO	NXDOESLA	NGLEYKNO	WABOUTTH
VH?DWKBFU	FPWNTDKI	YCUQZERE	EVLDKFEZ	MOQQJLTT
IS?THEYSH	OULDITSB	URIEDOUT	THERESOM	EWHEREXW
UGSYQPFE	UNLAVIDX	FLGGTEZ?F	KZBSFDQV	GOGIPUFX
HOKNOWST	HEEXACTL	OCATION?O	NLYWWTHI	SWASHISL
HHDRKFFH	QNTGPUAE	CNUVPDJM	QCLQUMUN	EDFQELZZ
ASTMESSA	GEXTHIRT	YEIGHTDE	GREESFIF	TYSEVENM
VRRGKFFV	OEXXBDMV	PNEQXEZL	GREDNQFM	PNZGLFLP
INUTESSI	XPOINTFI	VESECOND	SNORTHSE	VENTYSEV

MRJQYALM GNUVPDXV KPDQUMZB EDMHDAFM JGZNUPLG
ENDEGREE SEIGHTMI NUTESFOR TYFOURSE CONDSWES

EWJLLAET G
TIDBYROW S

~~(FOUO)~~ Respaced and punctuated, it reads:

"IT WAS TOTALLY INVISIBLE. HOW'S THAT POSSIBLE? 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 THE EXACT LOCATION? ONLY W.W. THIS WAS HIS LAST TRANSMISSION. THIRTY-EIGHT DEGREES, FIFTY-SEVEN MINUTES, SIX POINT FIVE SECONDS NORTH. SEVENTY-SEVEN MINUTES, FORTY-FOUR SECONDS WEST. I.D. BY ROWS."

(sg) Note: W.W. is presumed to be William Webster. The coordinates refer to the location of or a location within the Central Intelligence Agency. The significance of I.D. BY ROWS remains undetermined.

PART 3

~~(S)~~

Cryptography: Keyed Columnar transposition
 Matrix size: Incompletely filled 4 X 86
 Specific key: **KRYPTOS**, numerically keyed and repeated 13 times
 (first 12 columns listed below)
 Route: Bottom to top

SLOWLYDESPARATLYSLOWLYTHEREMAINSOFPASSAGEDE
 ASREMOVEDWITHTREMBLINGHANDSIMADEATINYBREACH
 OLEALITTLEIINSERTEDTHECANDLEANDPEEREDINTHEH
 FLICKERBUTPRESENTLYDETAILSOFTHEROOMWITHINEM

1	1	1	9	8	7
2	1	0			

BRISTHATENCUMBEREDTHELOWERPARTOFTHEDOORWAYW
 INTHEUPPERLEFTHANDCORNERANDTHENWIDENINGTHEH
 OTAIRESCAPINGFROMTHECHAMBERCAUSEDTHEFLAMETO
 ERGEDFROMTHEMISTXCANYOUSEEANYTHINGQ

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

(U) "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"

Note: The above is a paraphrase from The Tomb of Tut-Ankh-Amen written by Mr. Howard Carter.