Kryptos

MATH3302 LECTURE, 2 APRIL 2019

RICHARD BEAN

Background

- ID360 “Cryptography” in 1995
- An “interdisciplinary” subject
- Mathematics and Computer Science
- Cryptography links to many areas of mathematics and CS
  - Number theory
  - Combinatorics
  - Statistics
  - Information theory
- Cryptanalysis – linguistics and psychology also help

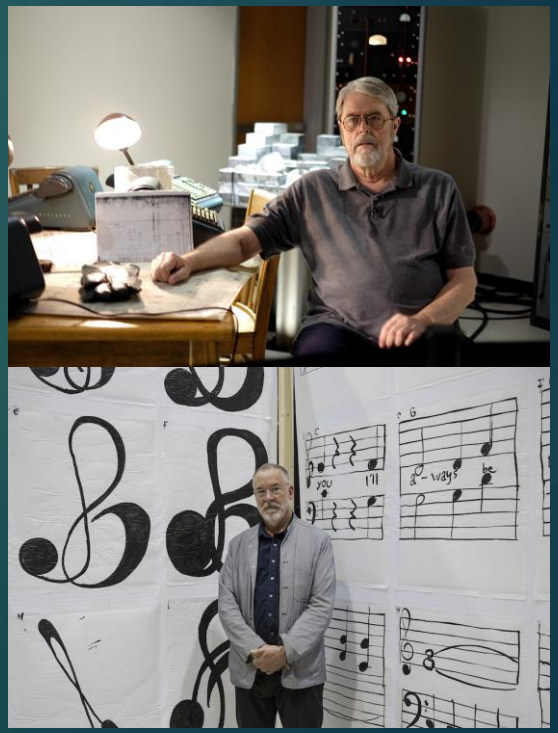
The prehistory of the Kryptos sculpture

- Office of Strategic Services (OSS) founded 1942 after Pearl Harbor
- Central Intelligence Agency (CIA) founded 1947 after WW2
- Original HQ built at Langley, Virginia in Nov 1959 – Mar 1961.

- Langley is a metonym for the CIA
- CIA Fine Arts Commission established in 1963
  - Purpose: "to advise the Director on esthetic matters relating to the Headquarters Building and grounds"
- New HQ built at Langley in May 1984 – Mar 1991
- "George Bush Center for Intelligence" (DCI 1976-77, named 1999)

Art selection for the new HQ

- General Services Administration "Art-in-Architecture" department chose artists for new building
- Criteria: "This art should reflect life in all its positive aspects (e.g. truth, justice, courage, liberty etc.) It should engender feelings of well-being, hope and promise and such."
- March 1988 – James Sanborn selected for sculpture and Matt Mullican for interior design. $450,000 total contract.
- April 1988 – Mullican declines. "When I think CIA, I think guns … I think international trauma. I think participating at the CIA would somehow imply my support for it. Context creates meaning."
- Sanborn "signed on immediately" saying "… something on this scale … transforms you financially." $250,000 contract.

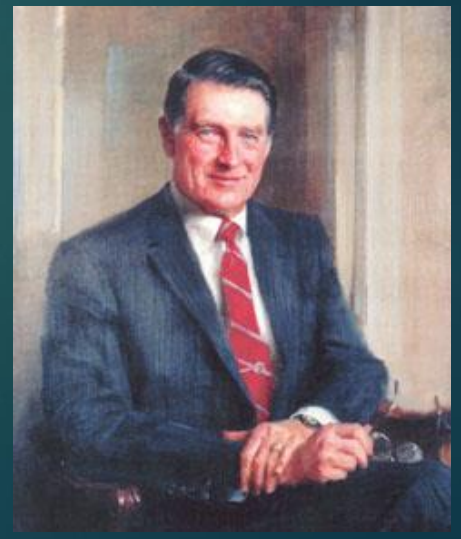


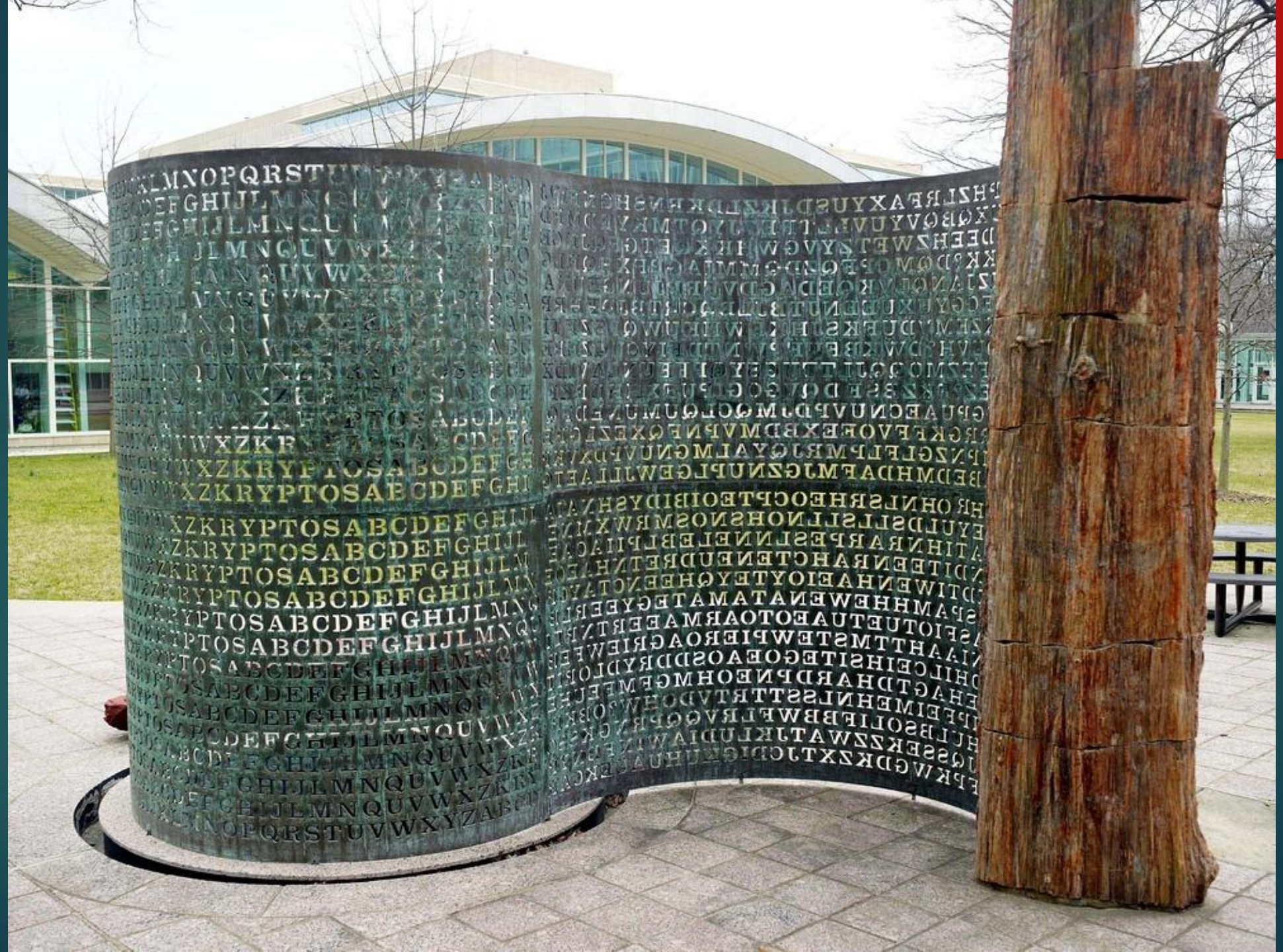
Creation (1988)

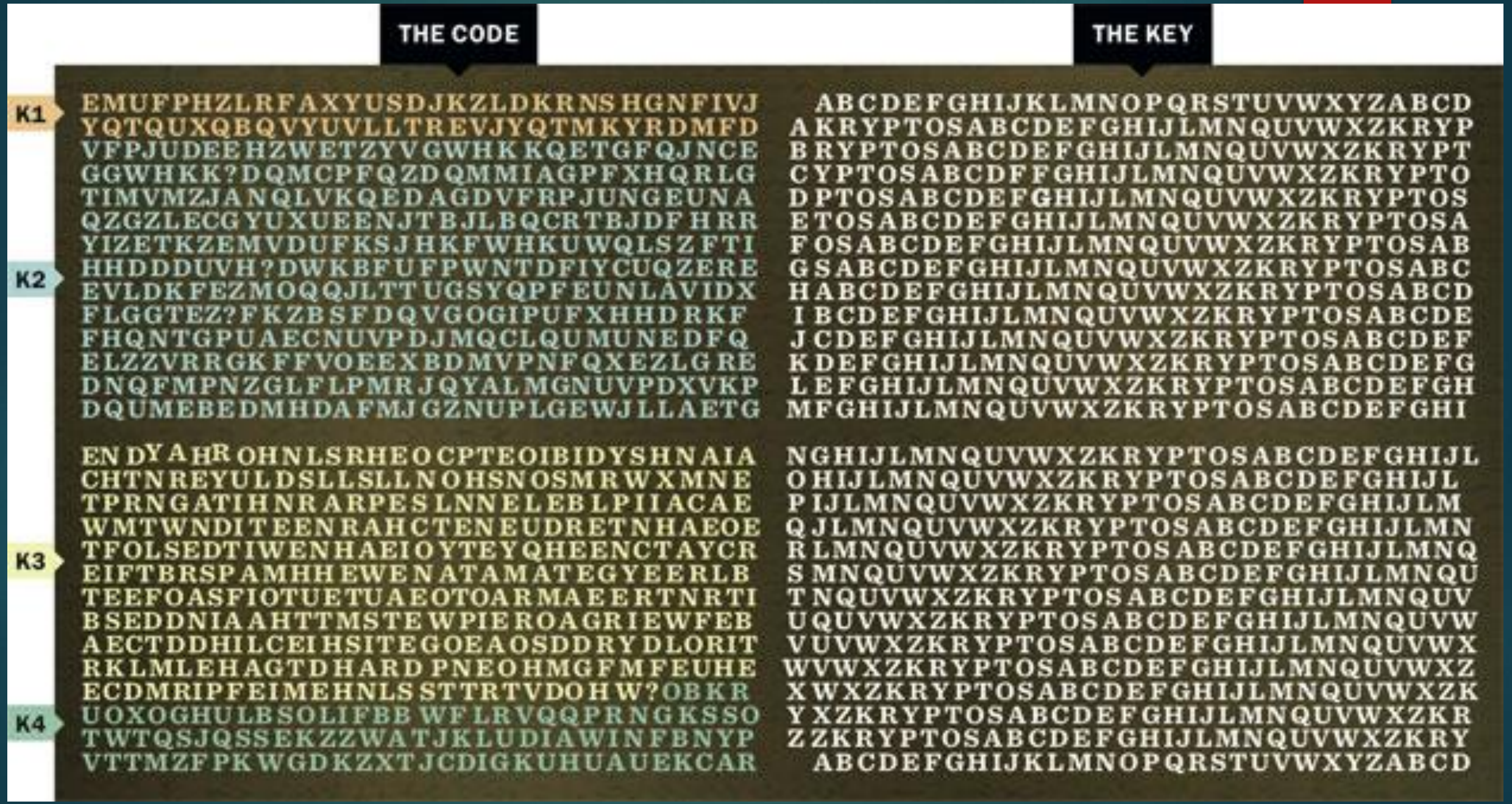
- November 1988 – model presented "a sculpture composed primarily of slabs of red granite, with verdigris copper plates (pierced by frequency code alphabet tables), lodestone, and petrified wood used as secondary materials."
- "Four aesthetically united sculptural groupings that are sophisticated, intellectual, and of a simple, strong, successful scale. It symbolizes time and change through the use of red granite, green quartz, alphabetical frequency tables carved out of copper, a meteorite, a lodestone, a petrified tree, specific plants, copper plates relating stories of natural events and possibly two shallow pools."

Creation (1990)

- *The secret phrase will be cut into the plate. Anyone who knows a coding system called the Vigenere Tableau, invented in 1586 by French diplomat Blaise de Vigenere, will be able to decipher one-half of the phrase. The other half will be encoded in* ***a modern system created for the project*** *by an expert cryptographer, whom Sanborn would not identify. (Washington Post, January 1990)*
- Sanborn worked with Edward Scheidt, a retired CIA cryptographer, in 1990, to design the code systems
- Dedication ceremony 3 November 1990. CIA Director William Webster: Kryptos "speaks to a sense of place … [Sanborn] has captured much of what this agency is about."

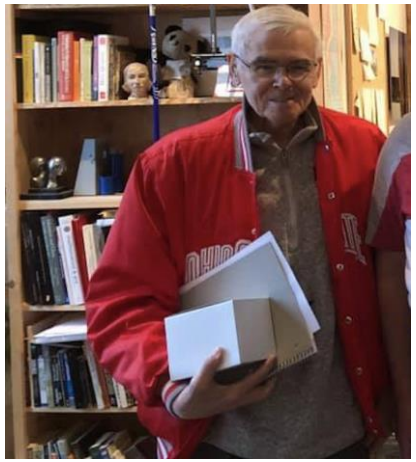



XZKRYPTOSABCDEFGHIJ
ZKRYPTOSABCDEFGHIJL
ZKRYPTOSABCDEFGHIJLM
RYPTOSABCDEFGHIJLMN
PTOSABCDEFGHIJLMNQ
TOSABCDEFGHIJLMNQU
OSABCDEFGHIJLMNQUV
SABCDEFGHIJLMNQUVW
ABCDEFGHIJLMNQUVWX
BCDEFGHIJLMNQUVWXZ
CDEFGHIJLMNQUVWXZK
DEFGHIJLMNQUVWXZKR
EFGHIJLMNQUVWXZKRY
FGHIJLMNQUVWXZKRYP
GHIJLMNQUVWXZKRYPT
HIJLMNQUVWXZKRYPTO
IJLMNQUVWXZKRYPTOS
JLMNQUVWXZKRYPTOSA
LMNQUVWXZKRYPTOSAB
MNQUVWXZKRYPTOSABC
NQUVWXZKRYPTOSABCD
QUVWXZKRYPTOSABCDE
UVWXZKRYPTOSABCDEF
VWXZKRYPTOSABCDEFG
WXZKRYPTOSABCDEFGH
XZKRYPTOSABCDEFGHI


THE CODE
THE KEY
K1
EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJ
YQTQUXQBQVYUVLLTREVJYQTMKYRDMFD
VFPJUDEEHZWETZYVGWHKKQETGFQJNCE
GGWHKK?DQMCPFQZDQMMIAGPFXHQRLG
TIMVMZJANQLVKQEDAGDVFRPJUNGEUNA
QZGZLECGYUXUEENJTBJLBQCRTBJDFHRR
YIZETKZEMVDUFKSJHKFWHKUWQLSZFTI
HHDDDUVH?DWKBFUFPWNTDFIYCUQZERE
K2
EVLDKFEZMOQQJLTTUGSYQPFEUNLAVIDX
FLGGTEZ?FKZBSFDQVGOGIPUFXHHDRKF
FHQNTGPUAECNUVPDJMQCLQUMUNEDFQ
ELZZVRRGKFFVOEEXBDMVPNFQXEZLGRE
DNQFMPNZGLFLPMRJQYALMGNUVPDXVKP
DQUMEBEDMHDAFMJGZNUPLGEWJLLAETG
ABCDEFGHIJKLMNOPQRSTUVWXYZABCD
AKRYPTOSABCDEFGHIJLMNQUVWXZKRYP
BRYPTOSABCDEFGHIJLMNQUVWXZKRYPT
CYPTOSABCDFFGHIJLMNQUVWXZKRYPTO
DPTOSABCDEFGHIJLMNQUVWXZKRYPTOS
ETOSABCDEFGHIJLMNQUVWXZKRYPTOSA
FOSABCDEFGHIJLMNQUVWXZKRYPTOSAB
GSABCDEFGHIJLMNQUVWXZKRYPTOSABC
HABCDEFGHIJLMNQUVWXZKRYPTOSABCD
IBCDEFGHIJLMNQUVWXZKRYPTOSABCDE
JCDEFGHIJLMNQUVWXZKRYPTOSABCDEF
KDEFGHIJLMNQUVWXZKRYPTOSABCDEFG
LEFGHIJLMNQUVWXZKRYPTOSABCDEFGH
MFGHIJLMNQUVWXZKRYPTOSABCDEFGHI
EN DY A HR OHNLSRHEO CPTEOIBIDYSHNAIA
CHTNREYULDSLLSLLNOHSNOSMRWXMNE
TPRNGATIHNRARPESLNNELEBLPIIACAE
WMTWNDITEENRAHCTENEUDRETNHAEOE
TFOLSEDTIWENHAEIOYTEYQHEENCTAYCR
K3
EIFTBRSPAMHHEWENATAMATEGYEERLB
TEEFOASFIOTUETUAEOTOARMAEERTNRTI
BSEDDNIAAHTTMSTEWPIEROAGRIEWFEB
AECTDDHILCEIHSITEGOEAOSDDRYDLORIT
RKLMLEHAGTDHARDPNEOHMGFMFEUHE
ECDMRIPFEIMEHNLSSTTRTVDOHW?OBKR
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
K4
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR
NGHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
OHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
PIJLMNQUVWXZKRYPTOSABCDEFGHIJLM
QJLMNQUVWXZKRYPTOSABCDEFGHIJLMN
RLMNQUVWXZKRYPTOSABCDEFGHIJLMNQ
SMNQUVWXZKRYPTOSABCDEFGHIJLMNQU
TNQUVWXZKRYPTOSABCDEFGHIJLMNQUV
UQUVWXZKRYPTOSABCDEFGHIJLMNQUVW
VUVWXZKRYPTOSABCDEFGHIJLMNQUVWX
WVWXZKRYPTOSABCDEFGHIJLMNQUVWXZ
XWXZKRYPTOSABCDEFGHIJLMNQUVWXZK
YXZKRYPTOSABCDEFGHIJLMNQUVWXZKR
ZZKRYPTOSABCDEFGHIJLMNQUVWXZKRY
ABCDEFGHIJKLMNOPQRSTUVWXYZABCD

Solutions to K1, K2, K3

- December 1992 - a team of National Security Agency (NSA) employees including Ed Hannon and Dennis McDaniels finds solutions to the first three sections
- February 1998 – David Stein of CIA finds solutions (pencil and paper only)
- June 1999 - Jim Gillogly solves K1-K3 and announces solutions on USENET newsgroup sci.crypt



Part Three

- Assume ciphertext divisions are known to save time here!
- Look at frequency table of letters – 336 letters

E	T	A	N	R	H	I	O	D	L	S	M	C	F	P	W	Y	B	G	U	K	Q	V	X
50	31	26	23	23	21	21	18	17	16	16	12	9	8	8	8	8	6	6	5	1	1	1	1

- Index of coincidence = $\frac{\sum_{i=1}^{n} f_n(f_n-1)}{n(n-1)} = \frac{7446}{336*335} = 0.06615$
- J and Z are missing
- The high-frequency letters ETAOIN SHRDLU are generally at the top, and JKQXZ are down the bottom
- Plaintext is English, method is some kind of transposition

Part Three

- Several different types of transposition encryption
  - Incompletely filled column transposition

M	O	N	A	R	C	H	Y
D	E	M	O	C	R	A	C
Y	I	S	T	H	E	B	E
S	T	R	E	V	E	N	G
E	B	E	N	A	Z	I	R
B	H	U	T	T	O		

A	C	H	M	N	O	R	Y
O	R	A	D	M	E	C	C
T	E	B	Y	S	I	H	E
E	E	N	S	R	T	V	G
N	Z	I	E	E	B	A	R
T	O		B	U	H	T	

  - Write off in five letter blocks: OTENT REEZO ABNID YSEBM …

Part three – NSA cryptanalysis

- NSA attack (December 1992)
  - https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cia-kryptos-sculpture/doc_7.pdf
  - The explanation given is that there was one "Q" in the 336 letters, which was paired with one of the five "U"s. Columns were filled in
  - Eventually, an incompletely filled 4 x 86 matrix was discovered
  - The explanation doesn't seem to make sense, because there's no Q followed by U in the plaintext

Part three – CIA cryptanalysis

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

4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96
5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	65	69	73	77	81	85	89	93	97
6	10	14	18	22	26	30	34	38	42	46	50	54	58	62	66	70	74	78	82	86	90	94	98
7	11	15	19	23	27	31	35	39	43	47	51	55	59	63	67	71	75	79	83	87	91	95	99
100	104	108	112	116	120	124	128	132	136	140	144	148	152	156	160	164	168	172	176	180	184	188	192
101	105	109	113	117	121	125	129	133	137	141	145	149	153	157	161	165	169	173	177	181	185	189	193
102	106	110	114	118	122	126	130	134	138	142	146	150	154	158	162	166	170	174	178	182	186	190	194
103	107	111	115	119	123	127	131	135	139	143	147	151	155	159	163	167	171	175	179	183	187	191	195
196	200	204	208	212	216	220	224	228	232	236	240	244	248	252	256	260	264	268	272	276	280	284	288
197	201	205	209	213	217	221	225	229	233	237	241	245	249	253	257	261	265	269	273	277	281	285	289
198	202	206	210	214	218	222	226	230	234	238	242	246	250	254	258	262	266	270	274	278	282	286	290
199	203	207	211	215	219	223	227	231	235	239	243	247	251	255	259	263	267	271	275	279	283	287	291
292	296	300	304	308	312	316	320	324	328	332	336												
293	297	301	305	309	313	317	321	325	329	333	1												
294	298	302	306	310	314	318	322	326	330	334	2												
295	299	303	307	311	315	319	323	327	331	335	3												

- CIA attack (1998)
  - https://kryptosinfo.files.wordpress.com/2009/06/kryptos-stein-cia.pdf
  - Supposedly, the 336 letter text was arranged into four blocks, 3 of size 96 and 1 of size 48 (336=96*3+48), with "END" at the end, and then the columns of each were permuted using digram frequencies to get plaintext
  - However, the diagrams have errors and are hard to follow e.g. first block has LLSL then HSNO SNRW XNNI TPRN …

Part three – Gillogly cryptanalysis

- http://www.thekryptosproject.com/kryptos/cia/thecryptogram/pdfs/Binder1.pdf
- Tried different kinds of transpositions with automated solver programs – Complete and Incomplete Columnar Transposition, Myszkowski, Railfence, Grilles, Route Transposition
- Eventually, found that double transposition with one period forced to length 8 works
- "Three route transpositions with different block sizes each consisting of writing it into rows of 14, 24 and 8 letters, then taking it off by columns in reverse order."

The encryption process

- The worksheets for both parts of the K3 encryption process have been released by Sanborn (2007 and 2013)
- http://kryptools.com/Sheets/sheets.htm
- Working from the sculpture text, write it into a 24x14 grid, bottom to top, left to right, starting in the bottom left hand corner

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

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

Simplest K3 encryption/decryption method

- Add the "?" to the end of the 336 characters, making a 337 character text
- 337 is a prime number
- Number the letters 0 to 336
- To decrypt, take every 192nd character (working modulo 337)
- To encrypt, take every 251st character (working modulo 337)
- This works as 192 and 251 are inverses in $\mathbb{Z}_{337}$

Cryptanalysis of K2

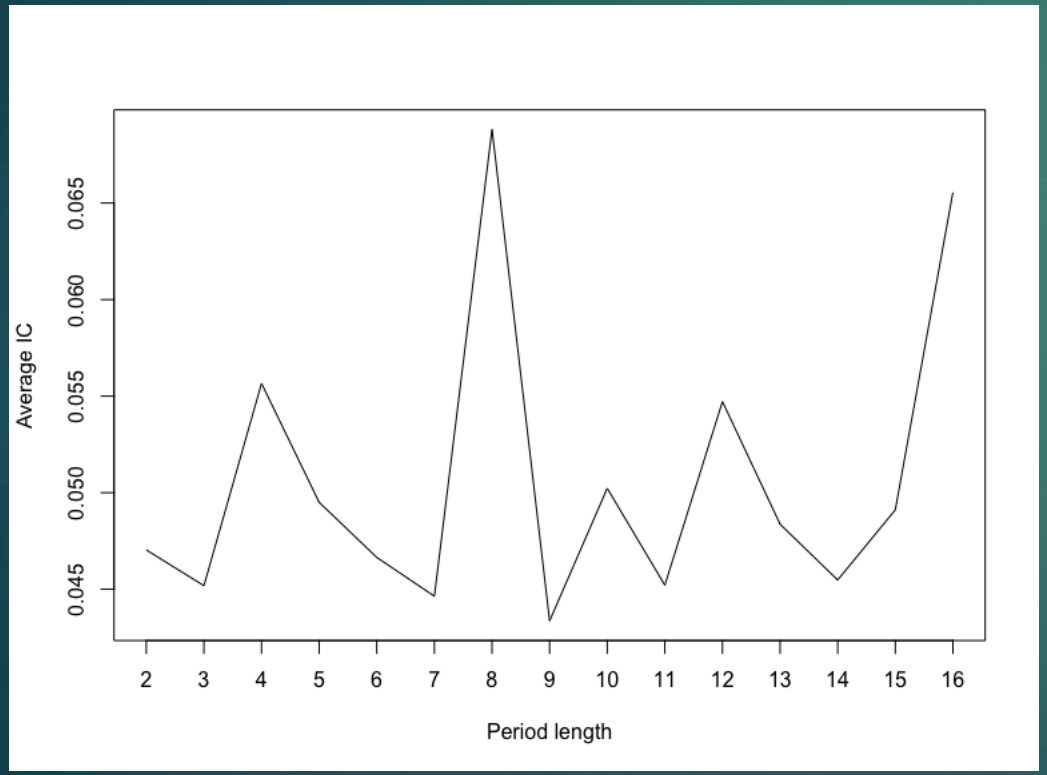
- First remove all the question marks "?"
- 369 letters = 3*3*41
- Letter frequency

E	F	D	Q	G	U	L	Z	M	V	K	N	P	H	J	T	R	A	W	B	C	I	X	Y	S	O
29	27	24	24	23	20	18	18	16	16	15	15	15	14	13	13	11	9	8	7	7	7	7	6	4	3

- Index of coincidence= $\frac{\sum_{i=1}^{n} f_n(f_n-1)}{n(n-1)} = \frac{6174}{336*335} = 0.04547$
- Not a transposition or monoalphabetic substitution
- Look for repeated ciphertext n-grams
- Numbering characters 1-369, GWHKK at positions 17, 33 and NUVPD at positions 258, 330. gcd(330-258,33-17)=8

Cryptanalysis of K2

- Probably some kind of polyalphabetic substitution with period 8
- Calculate average indices of coincidences of the columns, after arranging texts into equal length rows




```
k2 <- "VFPJUDEEHZWETZYVGWHKKQETGFQJNCEGGWHKKDQMCPFQZDQMMIAGPFXHQRLGTIMVMZJANQLVKQEDAGDVFRPJUNGEUNAQZGZLECGYU)
ic <- function(s) {
  n <- utf8ToInt(s)
  l <- nchar(s)
  co <- as.numeric(table(n[n>=65]))
  return(sum(co*(co-1))/l/(l-1))
}
ic2 <- function(s,n,o)
{
  return(ic(paste(unlist(strsplit(s,""))[[1]][seq(0,(trunc(nchar(s)/n))*n,n)+o+1]),sep="",collapse="")))
}

ik <- function(n)
{
  ic3 <- function(m)
  {
    return(ic2(k2,n,m));
  }
return(mean(unlist(lapply(0:(n-1),ic3))));
}

plot(1:20,lapply(1:20,ik),xaxt='n',type='l',xlab="Period length",ylab="Average IC")
axis(1,at=1:20)
```

Cryptanalysis of K2

- http://scienceblogs.de/klausis-krypto-kolumne/2015/11/23/verschluesselung-auf-kryptos-modell-geknackt/
- Ed Scheidt provided a "mini-Kryptos" sculpture in 2015 to illustrate polyalphabetic encryption using the keyword"RUG"
- First row of ciphertext is TIJVMSRSHVXOMCJVXOENA

Polyalphabetic decryption, keyword RUG

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
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
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
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
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
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
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
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
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
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
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
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
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

Codes may be divided into two different classes — namely, substitutional and transpositional types (the transpositional being the hardest to decipher without the key).

K2 Keyword determination

- Gillogly: found by trying polyalphabetic cipher types (Vigenere, Beaufort, Variant Beaufort, Porta), then finally "Quagmire"
- Writing the "KRYPTOS" alphabet as the top row and using an algorithm "shotgun hillclimbing" (also known as "random restart" hillclimbing)
- Scoring the result by sum of logged n-gram frequencies
- Keyword: "ABSCISSA"
- Plaintext: *It was totally invisible. How's 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 WW. This was his last message: x Thirty-eight degrees fifty-seven minutes six point five seconds North, seventy-seven degrees eight minutes forty-four seconds West. ID by rows.*
- In 2006, Sanborn said plaintext was intended to read "X LAYER TWO" instead of "ID BY ROWS" at end

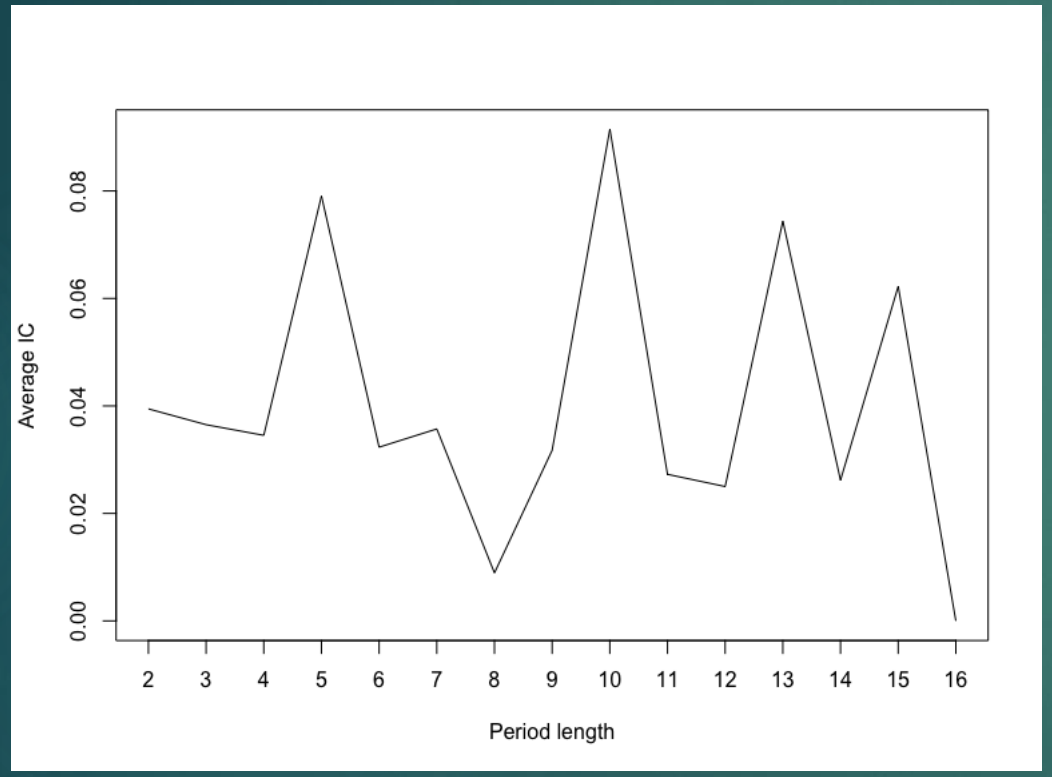
Cryptanalysis of K1

- Letter frequency table

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

- Index of coincidence= $\frac{\sum_{i=1}^{n} f_n(f_n-1)}{n(n-1)} = \frac{148}{63*62} = 0.03789$
- Almost exactly 1/26=0.03846
- Not a transposition or monoalphabetic substitution
- Look for repeated ciphertext n-grams
- VJYQT at positions 31 and 51; ZL at 7 and 19; YU at 13 and 43

Cryptanalysis of K1



- Hill climbing with keywords of length 10 leads to the keyword "PALIMPSEST"
- Plaintext: "*Between subtle shading and the absence of light lies the nuance of iqlusion.*"
- Initials of plaintext anagram to "LOSS BATTALION"

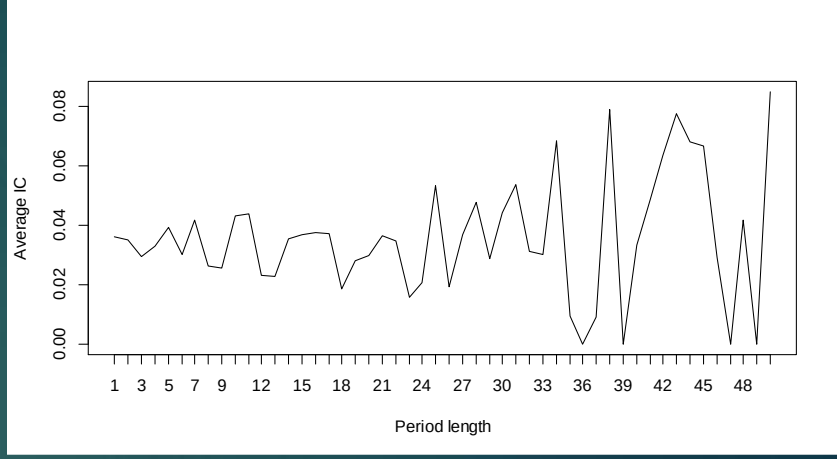
K4

```
------------------------?OBKR
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR
```

- "A whole different ballgame" of multiple codes written by a retired CIA cryptographer (Sanborn 1991)

- Scheidt 2005: *There are four different processes. Two of them are similar and the other two are different things. The first three processes were designed so that a person could, through cryptographic analysis, have access to the English language (on the sculpture). And the last process, I masked the English language so it's more of a challenge now. It's progressively harder in the challenges. All four (sections) are done in the English language. The message could have been in another language. (But) this particular puzzle is in the English language.... The techniques of the first three parts, which some people have broken, (used) frequency counting and other techniques that are similar to that. You can get insight into the sculpture through that technique because the English language is still visible through the code. (But with) this other technique (in the fourth part), I disguise that. So ... you need to solve the technique first and then go for the puzzle. The masking technique may not be known.*

K4 basic analysis



- Index of coincidence = $\frac{\sum_{i=1}^{n} f_n(f_n-1)}{n(n-1)} = \frac{336}{97*96} = 0.03608 \cong 1/26$
- Letter frequencies

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

- Interesting that K, T, O, S are near the top here
- K1 ciphertext missing C, O, W; K3 CT missing J, Z; K2 and K4 CT have all letters
- K1 plaintext missing J,K,M,P,R,V,X,Y,Z; K2 PT J,Q,Z; K3 PT J,Z
- Slight IC peaks at width 25, 50

K4 hints released

- November 2010 – "NYPVTT" in positions 64-69 of the ciphertext decrypts to "BERLIN"; also K1 and K2 sheets released indicating "IQLUSION" was a mistake caused by misspelling "PALIMPSEST" keyword
- November 2014 – "MZFPK" in positions 70-74 of the ciphertext decrypts to "CLOCK"
- 2019 – another clue to be released

K4 ideas

- Thematically, if K1 and K2 are substitution and K3 is transposition, then K4 could be a combination of both in some order
- If K4 includes the "?" then it is 27 different characters, which is like the "Trifid" cipher; fits in with "historical progression of ciphers" in sculpture, but very well-known cipher susceptible to hill-climbing attacks
- "Gromark" using the coordinates in the K2 plaintext as a numeric key. But, this is also a well-known "ACA" cipher.
- "Hill Cipher" – since Sanborn mentions "matrix codes" often, and "HILL" is in the "tabula recta". However, Sanborn has said he's an "anathemath", the ciphertext has a prime number of letters, and exhaustive search using the "BERLINCLOCK" crib shows it's not a Hill cipher with matrix size 2. Unlikely.

Coincidences and "the pathology of cryptology"

- "A hidden code can be found almost anywhere, provided that one looks for it in a suitable manner." (Schmeh)
- The Baconian theory of Shakespeare – Elizabeth Wells Gallup and the Friedmans
- The "Bible Codes"
- Harold Gans, NSA

A priori and a posteriori analysis (Barry Simon, "*A Skeptical Look at the Torah Codes*")

- *One statistician I know who consults for various companies to analyze their data told me that whenever he starts a project for a new client he warns them that he's glad to discuss the way he's going to analyze the data in detail before he does the analysis. But once he does the analysis, he's not going to go back in response to - "why don't you try looking at it in thus and such a way". Because he guarantees that if you reanalyze it often enough, you can make the analysis show whatever you want.*
- *The point is that even well intentioned people if they keep reanalyzing data by changing the methods can produce results that aren't statistically valid.*

“Masquerade” by Kit Williams

- The original “Treasure Hunt” book, published August 1979, hint given December 1980, treasure found March 1982
- http://www.planetslade.com/masquerade.html
- *[Tony Bennett of GCHQ] had discovered even more exciting confirmation. Taking the numbers 1, 2, 3, 4, 5 from the Penny-Pockets square, and using the numbers in the same squares on the final page of the book, he came up with a sequence 10 46 4 7 5. By adding the 4 and the 6, he turned this into 10 10 4 7 5. He now told the astonished army of Parracks and Bennetts to turn back to the zodiac page, the one which had put them on to Gemini. He used his sequences of numbers to count through the letters on that page, starting at the end and going anti-clockwise. The last letter is G: 10 back from that gave E: another 10 came to M: 4 more to I: 7 to N: and the final 5 to I. Gemini again! It was indeed an astonishing coincidence.*
- ***G**SUN**I**OJDNA**E**KILUOYFIE**M**ITN**I**EC**N**AD*

Using the crib to find an algorithm which produces the crib

- Crib means known plaintext – here at a known position
- In June 2013, R. Scott Perry found: first decrypt using Quagmire III and with key EMUFPHZLRFA (the first eleven letters from K1) and the KRYPTOS alphabet, then transpose the result using the linear congruence 77+38x mod 97. Get BERLIN at the correct position (letters 64-69).

Matrix of width 7

- Arrange text in a 14x7 matrix
- Five of the six digram repeats are aligned in the same column

?	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	I
Q	S	S	E	K	Z	Z
W	A	T	I	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

Matrix of width 21

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	I	Q
S	S	E	K	Z	Z	W	A	T	I	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								

- Looking at pairs in the columns (i.e. considering rows 1/2, 2/3, 3/4, 4/5)
- We have 76 digrams. Of these 11 occur twice (AZ BS IT LS LW PK QZ SN WA ZT KK).
- In a 97-character random text, this happens about 1 in 1,500 times
- Permuting K4 randomly, i.e. retaining the letter frequency counts, this occurs about 1 in 6,600 times

The difficulty with K4

- The short length means that it is hard to find patterns and hard to know if observed patterns are "genuine" or just coincidences
- "*… if you have an unknown algorithm, a short plaintext, and only one message, that there has to be some hint as to what the algorithm is. If someone posted an unknown algorithm cipher challenge here with ~100 characters of ciphertext with no clue as to the algorithm, no one would even bother.*"
- The short length means that algorithms which would usually help diagnose a (known) cipher method don't work
- There's not much message context
- The algorithm may not be known
- We are essentially relying on Sanborn and Scheidt that no mistake has been made in the enciphering process

Last words

- *"Like Kryptos, the other public works are designed to exude their information slowly. ... For the past 30 years, my task as an artist has been to release this hidden information at a rate commensurate with its importance, and at the time of my choosing so as to prolong the experience of discovery. As we all know, artwork that gives up its form or content quickly is soon forgotten." (Sanborn 2012)*