KRYPTOS

Patrick Kellogg

patrickkellogg@gmail.com

http://www.patrickkellogg.com/kryptos

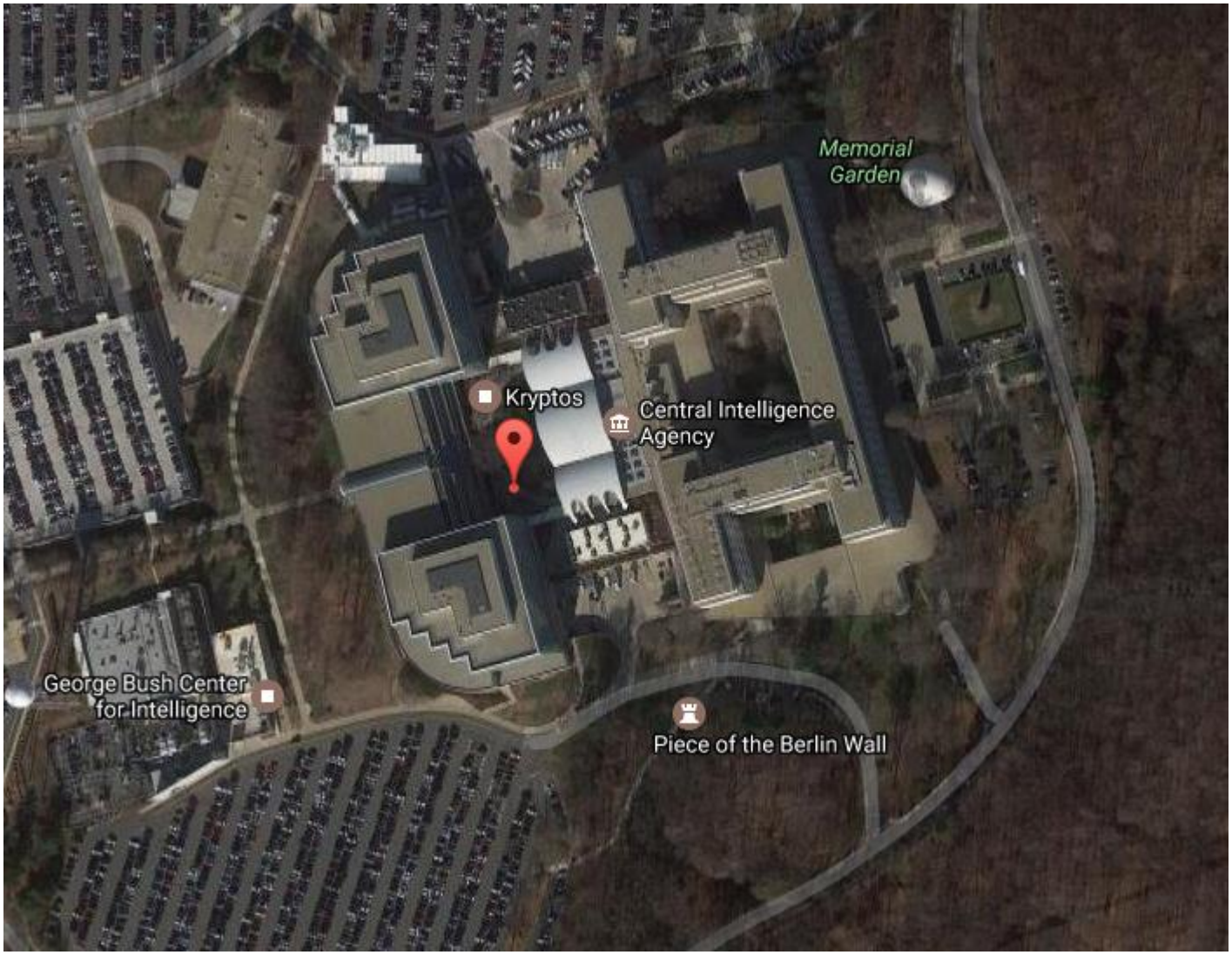
- I love this sculpture by Jim Sanborn

(Note: tiny reproduction)

About Kryptos

- The sculpture was erected in 1990 on the grounds of the CIA headquarters in Langley, Virginia
- The main part of the sculpture is a curved metal wall standing about 12 feet high
- There are also several benches, a fish pond, a magnetic lodestone, a compass, and many copper plates embossed with Morse code
- Sanborn worked with NSA cryptographer Ed Scheidt to understand the algorithms used

- (Note: not my photo. This is from Wikipedia, and taken was provided by the artist Jim Sanborn)



- Arial map from Google Earth

- The sculpture has encrypted text on the left side, and a Vigenère table on the right

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

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCD
AKRYPTOSABCDEFGHIJLMNQUVWXZKRYP
BRYPTOSABCDEFGHIJLMNQUVWXZKRYPT
CYPTOSABCDEFGHIJLMNQUVWXZKRYPTO
DPTOSABCDEFGHIJLMNQUVWXZKRYPTOS
ETOSABCDEFGHIJLMNQUVWXZKRYPTOSA
FOSABCDEFGHIJLMNQUVWXZKRYPTOSAB
GSABCDEFGHIJLMNQUVWXZKRYPTOSABC
HABCDEFGHIJLMNQUVWXZKRYPTOSABCD
IBCDEFGHIJLMNQUVWXZKRYPTOSABCDE
JCDEFGHIJLMNQUVWXZKRYPTOSABCDEF
KDEFGHIJLMNQUVWXZKRYPTOSABCDEFG
LEFGHIJLMNQUVWXZKRYPTOSABCDEFGH
MFGHIJLMNQUVWXZKRYPTOSABCDEFGHI
```

```
ENDYAHROHNLSRHEOCPTEOIBIDYSHNAIA
CHTNREYULDSLLSLLNOHSNOSMRWXMNE
TPRNGATIHNRARPESLNNELEBLPIIACAE
WMTWNDITEENRAHCTENEUDRETNHAEOE
TFOLSEDTIWENHAEIOYTEYQHEENCTAYCR
EIFTBRSPAMHHEWENATAMATEGYEERLB
TEEFOASFIOTUETUAEOTOARMAEERTNRTI
BSEDDNIAAHTTMSTEWPIEROAGRIEWFEB
AECTDDHILCEIHSITEGOEAOSDDRYDLORIT
RKLMLEHAGTDHARDPNEOHMGFMFEUHE
ECDMRIPFEIMEHNLSSTTRTVDOHW?OBKR
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR
```

```
NGHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
OHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
PIJLMNQUVWXZKRYPTOSABCDEFGHIJLM
QJLMNQUVWXZKRYPTOSABCDEFGHIJLMN
RLMNQUVWXZKRYPTOSABCDEFGHIJLMNQ
SMNQUVWXZKRYPTOSABCDEFGHIJLMNQU
TNQUVWXZKRYPTOSABCDEFGHIJLMNQUV
UQUVWXZKRYPTOSABCDEFGHIJLMNQUVW
VUVWXZKRYPTOSABCDEFGHIJLMNQUVWX
WVWXZKRYPTOSABCDEFGHIJLMNQUVWXZ
XWXZKRYPTOSABCDEFGHIJLMNQUVWXZK
YXZKRYPTOSABCDEFGHIJLMNQUVWXZKR
ZZKRYPTOSABCDEFGHIJLMNQUVWXZKRY
ABCDEFGHIJKLMNOPQRSTUVWXYZABCD
```

- There are actually four separate encrypted parts: the first three have been solved

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

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCD
AKRYPTOSABCDEFGHIJLMNQUVWXZKRYP
BRYPTOSABCDEFGHIJLMNQUVWXZKRYPT
CYPTOSABCDEFGHIJLMNQUVWXZKRYPTO
DPTOSABCDEFGHIJLMNQUVWXZKRYPTOS
ETOSABCDEFGHIJLMNQUVWXZKRYPTOSA
FOSABCDEFGHIJLMNQUVWXZKRYPTOSAB
GSABCDEFGHIJLMNQUVWXZKRYPTOSABC
HABCDEFGHIJLMNQUVWXZKRYPTOSABCD
IBCDEFGHIJLMNQUVWXZKRYPTOSABCDE
JCDEFGHIJLMNQUVWXZKRYPTOSABCDEF
KDEFGHIJLMNQUVWXZKRYPTOSABCDEFG
LEFGHIJLMNQUVWXZKRYPTOSABCDEFGH
MFGHIJLMNQUVWXZKRYPTOSABCDEFGHI
```

```
ENDYAHROHNLSRHEOCPTEOIBIDYSHNAIA
CHTNREYULDSLLSLLNOHSNOSMRWXMNE
TPRNGATIHNRARPESLNNELEBLPIIACAE
WMTWNDITEENRAHCTENEUDRETNHAEOE
TFOLSEDTIWENHAEIOYTEYQHEENCTAYCR
EIFTBRSPAMHHEWENATAMATEGYEERLB
TEEFOASFIOTUETUAEOTOARMAEERTNRTI
BSEDDNIAAHTTMSTEWPIEROAGRIEWFEB
AECTDDHILCEIHSITEGOEAOSDDRYDLORIT
RKLMLEHAGTDHARDPNEOHMGFMFEUHE
ECDMRIPFEIMEHNLSSTTRTVDOHW?OBKR
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR
```

```
NGHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
OHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
PIJLMNQUVWXZKRYPTOSABCDEFGHIJLM
QJLMNQUVWXZKRYPTOSABCDEFGHIJLMN
RLMNQUVWXZKRYPTOSABCDEFGHIJLMNQ
SMNQUVWXZKRYPTOSABCDEFGHIJLMNQU
TNQUVWXZKRYPTOSABCDEFGHIJLMNQUV
UQUVWXZKRYPTOSABCDEFGHIJLMNQUVW
VUVWXZKRYPTOSABCDEFGHIJLMNQUVWX
WVWXZKRYPTOSABCDEFGHIJLMNQUVWXZ
XWXZKRYPTOSABCDEFGHIJLMNQUVWXZK
YXZKRYPTOSABCDEFGHIJLMNQUVWXZKR
ZZKRYPTOSABCDEFGHIJLMNQUVWXZKRY
ABCDEFGHIJKLMNOPQRSTUVWXYZABCD
```

- The fourth part is still unencrypted! Despite many attempts over the last 25 years, no one knows what the last part of the message means, or if it ties the message of the whole sculpture together.

OBKR
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR

K1 Information

- The four parts of the sculpture have been referred to as K1, K2, K3, and K4
- K1 and K2 were first solved publicly in 1999 by computer scientist Jim Gillogly
- (Though supposedly the NSA solved it in three days)

K1 Solution

- K1 is a simple Vigenère substitution
- The keyword for K1 is PALIMPSEST
- And the plaintext for K1 turns out to be:

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

Weird Things About K1

- Sanborn intentionally misspelled the word "IQLUSION", which is a traditional method of making decryption more difficult

- The word "PALIMPSEST" means "a manuscript page, either from a scroll or a book, from which the text has been scraped or washed off so that the page can be reused for another document", which may have artistic meaning for the artist

More Weird Things About K1

- Note that the Vigenère used to solve K1 is not the one on the right side of the sculpture!

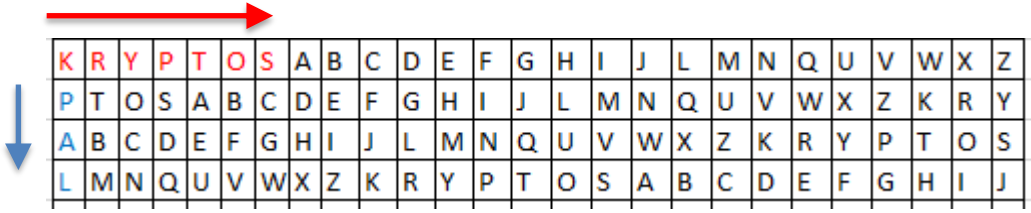
- Instead, Sanborn uses a variant of Vigenère called a “Quagmire III” which requires both an “Alphabet Key” at the top of the table, and a repeated “Passphrase”
  - Alphabet key = KRYPTOS
  - Passphrase = PALIMPSEST

Setting Up The Quagmire III

- First, take the standard alphabet and pull the non-repeating letters of the Alphabet Key out and stick them at the front

  KRYPTOSABCDEFGHIJLMNQUVWXZ

- Then, add rows corresponding with the Passphrase. For example, the first “P” row starts with “PTOSABC…”



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
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	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S
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

Warning: Actually Not A Vigenère

- However, Sanborn does something strange
- On the sculpture, he depicts a standard table. However, that is not the table he uses!

	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	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
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
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
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
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

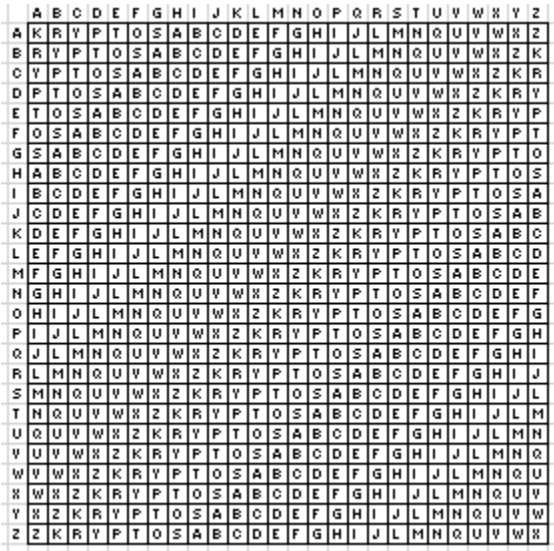
First lines on the sculpture ↑

	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
A	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
B	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
C	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
D	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
E	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

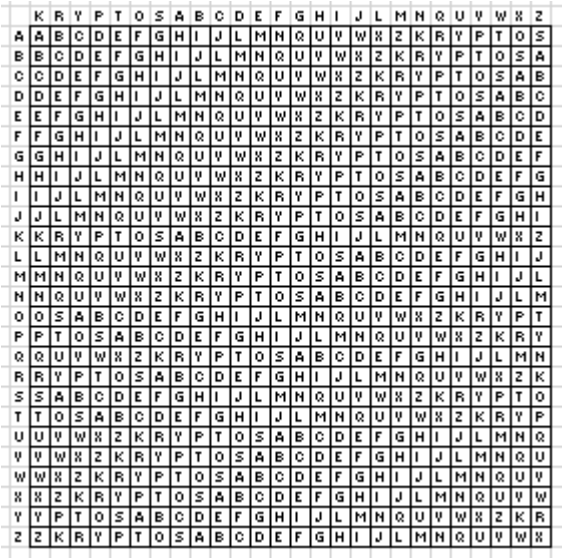
Actual substitution table ↑

“Sanborn” Vigenère Vs. Quagmire III

- Both the column order AND the row orders are different. This will give you incorrect results if you try to use a traditional method!



	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	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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



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

Standard Vigenère Sanborn’s Table

Let's Solve K1!

- EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJ YQTQUXQBQVYUVLLTREVJYQTMKYRDMFD
- So, the first two decrypted letters are "BE"

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
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	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S
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
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	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	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
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
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
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
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
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	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S
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

- The next are "TWEE"

More About K1

- BETWEEN SUBTLE SHADING AND THE ABSENCE OF LIGHT LIES THE NUANCE OF IQLUSION
- This is a poetic phrase made up by Jim Sanborn
- Maybe it refers to the nearby sundial?

  Or perhaps Sanborn is talking about the way the sun shines THROUGH the cut-out letters of the sculpture to cast a message on the world below

Let's Solve K2!

- K2 was solved similarly using the keyword

ABSCISSA

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
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
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
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
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
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
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	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O
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	J	L	M	N	Q	U	V	W	X	Z	K	R	Y	P	T	O	S
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
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

Let's Solve K2!

- The decrypted message is:

IT WAS TOTALLY INVISIBLE HOWS THAT POSSIBLE ? THEY USED THE EARTHS MAGNETIC FIELD X THE INFORMATION WAS GATHERED AND TRANSMITTED UNDERGRUUND TO AN UNKNOWN LOCATION X DOES LANGLEY KNOW ABOUT THIS ? THEY SHOULD ITS 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 X LAYER TWO

K2 Meaning

- This is another original message by Sanborn
- The geographic coordinates mentioned in the message correspond roughly to the location of the sculpture itself (about 100 feet southeast)
- No, the CIA won’t let you into the courtyard in order to dig around to see what you find

Weird things about K2

- Again, there is a misspelled word (UNDERGRUUND)

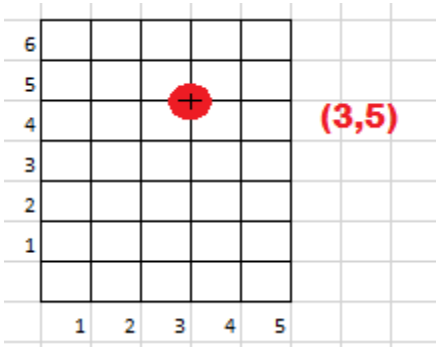
- In addition, K2 is the only part of the sculpture that contains punctuation (i.e. question marks). Traditionally, these are taken out before encryption

“Who is WW?”

- “WW” stands for William Webster, who was the Director of the CIA at the time that Kryptos was installed
- At the 1990 dedication ceremony of Kryptos, Sanborn gave a sealed envelope to Webster, which reportedly contained the solution
- However, in a 2005 interview with Wired magazine, Sanborn said that Scheidt and Webster only thought they knew the solution. In fact, he had deceived them.

More About K2

- The word “ABSCISSA” means:
  - the number whose absolute value (modulus) is the perpendicular distance of a point from the vertical axis
  - For example, below the “abscissa” is 3 and the “ordinate” is 5



- Maybe, like PALIMPSEST, this word has special meaning to the artist

Huge Mistake In K2

- The first people to solve K2 decrypted the final line to be: "...FOUR SECONDS WEST ID BY ROWS"
- However, this was wrong. It should have been "...FOUR SECONDS WEST X LAYER TWO"
- Sanborn made a terrible mistake when manufacturing the sculpture. He took the line

…PLGEXWJLLAETG

and bizarrely removed the the "X" thinking it was not needed. Of course, this dramatically changes the plaintext. If you randomly delete a letter in an encrypted Vigenère, all letters after it will be incorrect. It's amazing that the rest of the message after the X made any sense!

K3

- The third part of the sculpture is completely different! Unlike K1 and K3, it is not a Vigenère (nor a Quagmire III)

- Instead, the letters are rearranged according to a Transposition Cypher. No letter substitution is performed… a “Q” in the cypher is a “Q” in the plaintext forever

Rearranging K3 (Step 1)

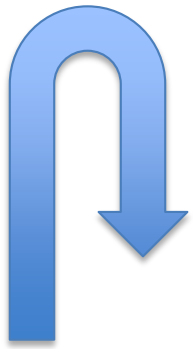
- First, put K3 into a 24 by 14 grid:

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

Rearranging K3 (Step 2)

- Then, rotate it clockwise 90 degrees:

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

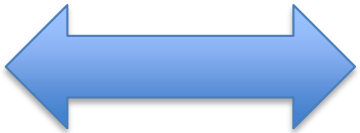


D	A	E	G	I	F	W	Q	E	W	R	N	D	E
M	G	G	R	B	I	E	H	O	N	A	O	Y	N
R	T	O	I	S	O	N	E	E	D	R	H	S	D
I	D	E	E	E	T	A	E	T	I	P	S	H	Y
P	H	A	W	D	U	T	N	F	T	E	N	N	A
F	A	O	F	D	E	A	C	O	E	S	O	A	H
E	R	S	E	N	T	M	T	L	E	L	S	I	R
I	D	D	B	I	U	A	A	S	N	N	M	A	O
M	P	D	A	A	A	T	Y	E	R	N	R	C	H
E	N	R	E	A	E	E	C	D	A	E	W	H	N
H	E	Y	C	H	O	G	R	T	H	L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

Rearranging K3 (Step 3)

- Reformat the result into an 8 by grid:

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



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

Rearranging K3 (Step 4)

- Finally, rotate the grid 90 degrees CW again:

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	N	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

K3 Solution

- 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 ?

More About K3

- This plaintext is a description of what happened when King Tut's tomb was opened in 1922, according to Howard Carter's book "The Tomb of Tutankhamun". Lord Carnarvon asked Carter if he saw anything peering into the tomb, and "Q" (Carter) famously responded, "wonderful things"!

- Note the misspelling of "DESPARATLY"

“How Did They Find The Solution?”

- Supposedly, NSA cryptographer Dennis McDaniels discovered the rotation in six hours by just sitting on his couch and looking at it
- He said he noticed a “Q” in the encrypted text and tried to manipulate the columns until a “U” appeared next to the “Q”
- (However, that story can’t be correct since there is on QU in the plaintext!)

How To Solve K4

- Nobody has solved K4 as of today (January 2017)
- Jim Sanborn was getting flooded with so many questions (and incorrect answers) that he implemented a website that would automatically check submissions at: http://www.kryptosclue.com
- However, as of 2017, that website is down and not functioning. You can supposedly test your answer by submitting $50 money order to Sanborn at: kryptos@earthlink.net
- Perhaps Sanborn is getting sick of the whole thing

Is K4 A Simple Transposition?

- Maybe K4 uses the same encryption method as K3, the way K1 and K2 are both Vigenère?
- However, this is doubtful
  - In English, the most frequently-used letters are:

    ETAOINSHRDLU…
  - However, for this message the most frequent are:

    K/STU/BO/AFGILQRWZ…
- So, K4 is probably not a single transposition

Is K4 A Simple Vigenère?

- In 2006, Jim Sanborn gave a clue:

The 64-69 letters in K4 are CLOCK

- And in 2014, he gave another clue:

The 70-74 letters are BERLIN

plaintext						b	e	r	l	i	n	c	l	o	c	k					
CIPHER	W	I	N	F	B	N	Y	P	V	T	T	M	Z	F	P	K	W	G	D	K	Z

- No one knows what a “BERLINCLOCK” is

Vigenère With BERLINCLOCK

- If we have the encrypted text and we know the solution plaintext, we can find the keyword!

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
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
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
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
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
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
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
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
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
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
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
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

KEY							E	L	Y	O	I	E	C	B	A	Q	K								
plaintext							b	e	r	l	i	n	c	l	o	c	k								
CIPHER	W	I	N	F	B	N	Y	P	V	T	T	M	Z	F	P	K	W	G	D	K	Z				

- Meaning the keyword would be ELYOIECBAQK, which makes no sense and can’t be right

Transposition AND A Vigenère

- My guess is that Sanborn used a transposition first (as in K3), and then did a substitution Vigenère (as in K1 and K2)

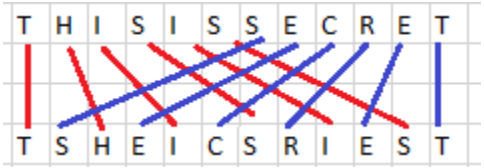
- Cracking a single Vigenère substitution is difficult. Decrypting a message that has used two (or more!) substitutions would be much worse. I am hoping that is not the case

Possible Method Of K4

- Take a message

T	H	I	S	I	S	S	E	C	R	E	T

- Create an interesting way of mixing it up

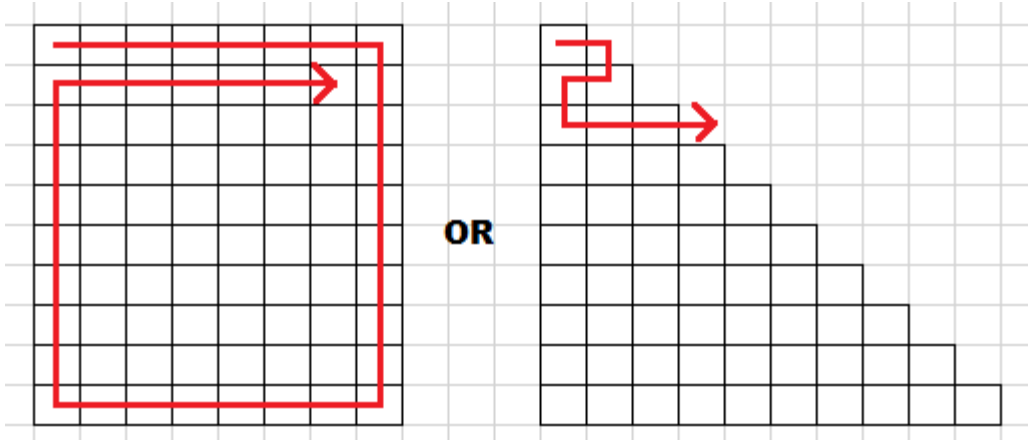


- Perform a Vigenère, using a keyword (like "SWAN")

KEY	S	W	A	N	S	W	A	N	S	W	A
plaintext	T	S	H	E	I	C	R	I	E	S	T
CIPHER	D	P	U	T	U	S	B	B	L	P	E

Methods Of Transformation

- Jim Sanborn is an artist. As such, he may have invented a new type of route or path transformation that looked “nice” to him



- Until the answer is discovered, we will not know

97 Is Prime

- Unfortunately, 97 is a prime number. So, it can't be factored in the many ways that K3 could (at 336 = 24 x 14 characters)
- K4 can't be arranged geometrically easily

  1+2+3+4+5+6+7+8+9+10+11+12+13=91

  1+3+5+7+9+11+13+15+17=81

  1+2+3+4+5+6+7+8+9+8+7+6+5+4+3+2+1=81

  1+3+5+7+9+11+13+11+9+7+5+3+1=85

Random Transformation

- So, my idea is to:
  1. Perform a random permutation on the 97 characters
  2. Use the BERLINCLOCK crib to find eleven letters that may be part of a keyword
  3. Use a dictionary lookup to see if any English word partially matches the keyword
- For example a partial decryption of BERLINCLOCK = KESLEAVIZLE might hint at a repeated keyword LEAVESLEAVESLEAVES

Example Of Method

- So, imagine that after shuffling all 97 letters of the encrypted text randomly, the 64th through 74th letters happen to be: BVABKKOSTKE

- Then, do a reverse "Sanborn's Vigenère" to find eleven keyword letters of KESLEAVIZLE

KEY			K	E	S	L	E	A	V	I	Z	L	E
plaintext			b	e	r	l	i	n	c	l	o	c	k
CIPHER	...	L	B	V	A	B	K	K	O	S	T	K	E	C	...

- A dictionary lookup suggests the keyword is LEAVES (repeated as LEAVESLEAVESLEAVES)

Python Code

- An implementation in Python can be found at: https://github.com/patrickkellogg/Kryptos
- Currently, the output states:
  1. How many of the 11 letters match the keyword
  2. The original encrypted 97 characters with the 11 chosen “crib” characters in UPPER CASE

```
Rating: 8 out of 11
obkruoxoghuLbsoLifbbwflrvqQprngkssotwtqSjqsSeKZZwatjkluDiawinfbn
ypvttmzfpkwgdKzxtjcdigkuhuauekCar
Groupit: ZKDCZKSQSLL
Segment: LICMDAWPRBL
Word: PROLICIDAL
DGWKSTWUCBKAOZBKOQHVHLPTLRDEQFTOSWJZWUBKSRFSNTGPYAJIRJERIUITVUWZ
KDCZKSQSLLTONMKXOFBPIGQNUAUFGKBAX
Period estimate:  2.12765957447
Strength:  7.67278771277
```

Code Results

3. “Groupit”, the 11 randomly shuffled encrypted letters that make up the BERLINCLOCK crib
4. “Segment”, the 11 possible keyword letters
5. The keyword chosen from a dictionary lookup
6. The fully decrypted string using the keyword
7. And finally, a FFT (described on next page)

```
Rating: 8 out of 11
obkruoxoghuLbsoLifbbwflrvqQprngkssotwtqSjqsSeKZZwatjkluDiawinfbn
ypvttmzfpkwgdKzxtjcdigkuhuauekCar
Groupit: ZKDCZKSQSLL
Segment: LICMDAWPRBL
Word: PROLICIDAL
DGWKSTWUCBKAOZBKOQHVHLPTLRDEQFTOSWJZWUBKSRFSNTGPYAJIRJERIUITVUWZ
KDCZKSQSLLTONMKXOFBPIGQNUAUFGKBAX
Period estimate:  2.12765957447
Strength:  7.67278771277
```

Fast Fourier Transform (FFT)

- If I have a good keyword candidate, I can see the locations of where chosen 11 crib letters came from

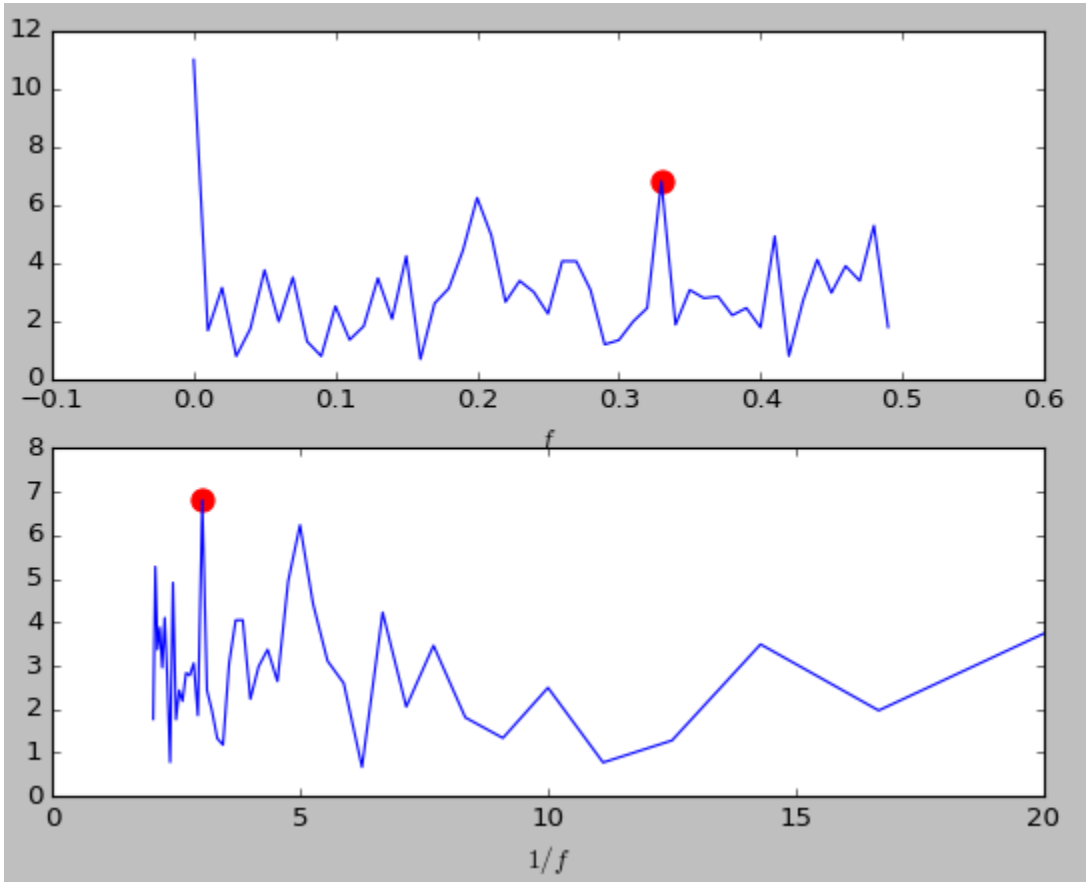
```
Rating: 9 out of 11
obKruOxoGhuLbsOliFbbWflR...
```

- In this example, every third letter seems to be randomly chosen to be part of the 11 letters
- This is turned into a Python array like this:

[0,0,1,0,0,1,0,0,1,0,0,1,0,0,1…

FFT Period Estimate

- Once I have a Python array of ones and zeros, I do a FFT on the data, and plot the results



FFT Strength

- Or, I could have done an autocorrelation. Both methods find repetitions in the data

```
Iteration: 1000 at 21:33:42 01/09/17 Eastern Standard Time
Rating: 8 out of 11
obkruoxOghuLbsolifbbwfLrvqQprngKssotwtqsJqssekzzwatjkludiawinfbnyPvttmZfpkwgdkzxTjcdigKuhuauEkcar
Groupit: ZPLETKKQOJL
Segment: LMJQIALPKAL
Word: PSALMODIAL
TSQZUIXFJIWYOFUBADUGGBSRDPRLLUZOTKVOWTSCTAUKJNWVRNHQSPEABSKXNZIZPLETKKQOJLRGWKFKCGTBODWKABQHMUIFS
Period estimate:  3.0303030303
Strength:  7.80980762949
```

- This keyword PSALMODIAL only has a Strength of 7.8, where better candidates are closer to 10. This keyword is probably not correct

More On The FFT

- I can also find the “peak” of the largest possible frequency component. For example,

```
Period estimate:  2.8641025641
Strength:  7.2235717908
```

might suggest a “folding” of every third letter

- This would be helpful in the future to try and figure out if and how Sanborn is perform a transformation.

My Word List

- Here are some possible keywords that my code has found:

PROLICIDAL
FOLDEDLY
FISHEATER
MOPISH
FRATCH
OBLIVIOUS
OBSIDIOUS
SUBCULTURE
SUPERIORLY
TWEEG
LOCKABLE
BRONTOLITE
FRANCOLITE
GEDECKTWORK
VULVOUTERINE
TOPSOIL
TABARET
STREPHOSYMBOLIA
KHUTBAH
SHERATON
PROTRACTIBLE
BUFOTALIN
POLYBASITE
SPITZ
ROUTINELY
FIBROMEMBRANE
UROLITH
POSTPAROXYSMAL
CLOGGER
SEMIFORMED
PROREBATE
SOLOTNIK
THULUTH
BRODEQUIN
CENTROSEMA
BASINET
SOMATOPHYTE
TURKOPHOBE
BUTTERFLY

Other Kryptos Errors

- There are several other strange things about the Kryptos sculpture:
  - The Vigenère table on sculpture (which, as stated, earlier, is not even used correctly by Sanborn for the encryption) has a bad line on the top line of the bottom-right quadrant "NGHIJL…" with one too many "L" characters at the end

- For some reason, in the bottom-left quadrant, three of the first few letters are raised above the others (the "YA R" in ENDYAHR)

- Some people have thought K4 contains an error and that's why it's difficult to crack, but in 2003 Sanborn said, "Yes. It ain't easy, but it's solvable!"

Quotes by Sanborn (Part 1)

- “The last 97 characters? Don't hold your breath… I saved the best for last.”

- “In a modern digital system, the 'key' is the keyword or number that you need to decrypt the message. Everyone knows the algorithm. It is just a black box into which you insert the key and the encrypted text, and the answer comes out the other end. In analog systems (as used in Kryptos) the 'key' is the algorithm.”

Quotes by Sanborn (Part 2)

- “I used a bit of stego (steganography) when designing the fourth part of Kryptos.”

- “In the first 3 parts, I gave anyone attempting to break the code the advantage of the English language with all its known patters(sic), but I removed that advantage in the fourth part.”

- “I don't presume to think that ‘Kryptos’ sculpture has the import that finding Tutankhamen's tomb would have, but it's that same magic of finding something, finding a fossil or finding an Indian arrow head or something like that. It's magical, because it's something that was made in the past. So I wanted to somehow demonstrate that magic, for everyone, once it was cracked."

Timeline

- 1988 Kryptos is commissioned by the CIA Fine Arts Commission
- 1990 Sculpture is installed at Langley, VA
- 2010 Sanborn gives out the crib “BERLIN”
- 2014 To honor the 25th anniversary of the fall of the Berlin Wall, the word “CLOCK” crib was given as a second crib

Ongoing Work

- Supposedly, the NSA stopped working on decrypting K4 because the small number of letters (97) were not enough to find an answer
- There has been a notable decrease of interest in the sculpture, and several websites have stopped updating progress and theories
- Even Jim Sanborn's own website no longer exists

My Future Work

- Refactor code so it can run faster, possibly even allowing multi-processors
- With a long list of strong keyword candidates, try to find possible methods Sanborn used for transformation. For example, if many keywords have period ≈ 3, then Sanborn probably used a grid of length or width of three (or a multiple of three)
- Look at alternative methods of rotation for K3

Resources

- http://www.elonka.com/kryptos
  - Elonka Dunin's Kryptos page. Probably the best collection of information on Kryptos available
- http://austininc.com/SciRealm/Kryptos.html
  - The webpage of John B. Wilson, a physicist and mathematician from North Carolina
- https://www.wired.com/2014/11/second-kryptos-clue/
  - Good article from "Wired" magazine from 2014
- https://en.wikipedia.org/wiki/Kryptos
  - Wikipedia, of course