Kryptos: A 29 year old mystery

Alfie Baines* — 170180540
a.e.baines@newcastle.ac.uk

School of Mathematics, Statistics and Physics
Supervisor: Dr Stuart Hall

Newcastle University

1. Aims

- To **automate** a majority of the **cryptanalysis** that has already been carried out on Kryptos
- To use **computing** to **decipher** the final section of Kryptos, known as **K4**

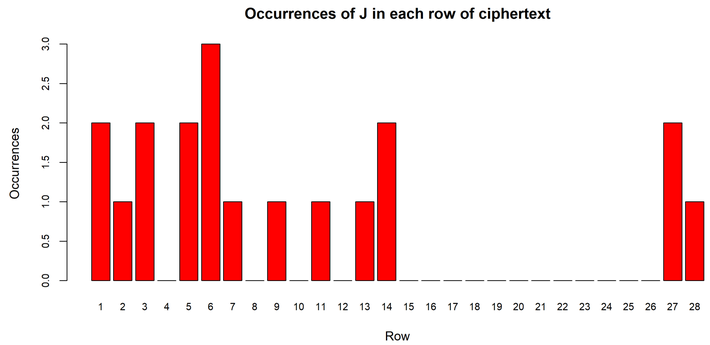
2. Transcript of Kryptos ciphertext

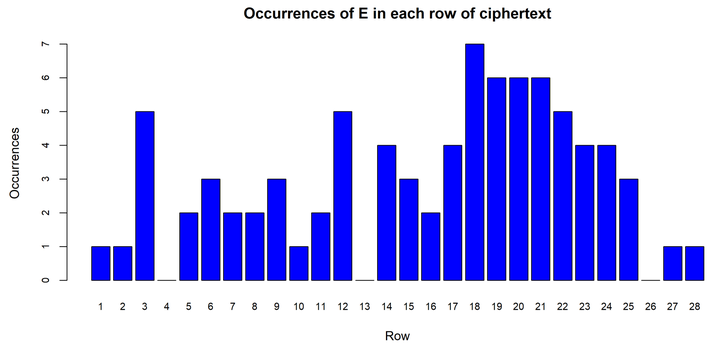
EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJ
YQTQUXQBQVYUVLLTREVJYQTMKYRDMFD
VFPJUDEEHZWETZYVGWHKKQETGFQJNCE
GGWHKK?DQMCPFQZDQMMIAGPFXHQRLG
TIMVMZJANQLVKQEDAGDVFRPJUNGEUNA
QZGZLECGYUXUEENJTBJLBQCRTBJDFHRR
YIZETKZEMVDUFKSJHKFWHKUWQLSZFTI
HHDDDUVH?DWKBFUFPWNTDFIYCUQZERE
EVLDKFEZMOQQJLTTUGSYQPFEUNLAVIDX
FLGGTEZ?FKZBSFDQVGOGIPUFXHHDRKF
FHQNTGPUAECNUVPDJMQCLQUMUNEDFQ
ELZZVRRGKFFVOEEXBDMVPNFQXEZLGRE
DNQFMPNZGLFLPMRJQYALMGNUVPDXVKP
DQUMEBEDMHDAFMJGZNUPLGEWJLLAETG
ENDYAHROHNLSRHEOCPTEOIBIDYSHNAIA
CHTNREYULDSLLSLLNOHSNOSMRWXMNE
TPRNGATIHNRARPESLNNELEBLPIIACAE
WMTWNDITEENRAHCTENEUDRETNHAEOE
TFOLSEDTIWENHAEIOYTEYQHEENCTAYCR
EIFTBRSPAMHHEWENATAMATEGYEERLB
TEEFOASFIOTUETUAEOTOARMAEERTNRTI
BSEDDNIAAHTTMSTEWPIEROAGRIEWFEB
AECTDDHILCEIHSITEGOEAOSDDRYDLORIT
RKLMLEHAGTDHARDPNEOHMGFMFEUHE
ECDMRIPFEIMEHNLSSTTRTVDOHW?OBKR
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR

- **K1** - Solved using **Vigenére** cipher: Keyword - **Palimpsest**
- **K2** - Solved using **Vigenére** cipher: Keyword - **Abscissa**
- **K3** - Solved using **Transposition** cipher
- **K4** - **UNSOLVED**

English alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Kryptos alphabet: KRYPTOSABCDEFGHIJLMNQUVWXZ

3. Frequency analysis





- By analysing how often letters appear in each row, it became obvious that the majority of rows 15-28 were written in English, but had been reordered - typical of a **Transposition Cipher**
- When comparing the frequency of letters in the green section to the typical letter frequencies of the English alphabet, it was almost identical

4. Vigenére cipher

The alphanumeric ordering of the Kryptos alphabet which is used when deciphering K1 and K2.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

If Σ is the alphabet of length l, with m being the length of the key, Vigenére encryption and decryption can be written;

$$C_i = E_K(M_i) = (M_i + K_{(i \bmod m)}) \bmod l \quad (1)$$

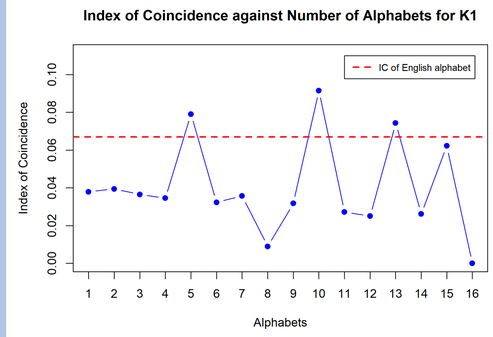
$$D_i = D_K(C_i) = (C_i - K_{(i \bmod m)}) \bmod l \quad (2)$$

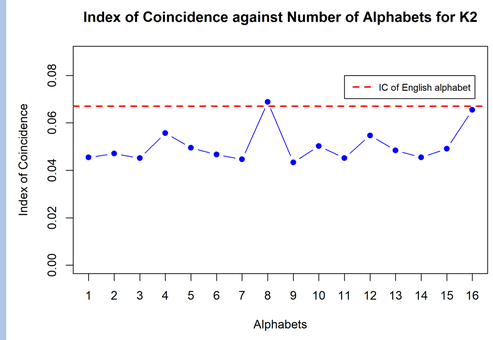
5. Index of coincidence

The **index of coincidence (IC)** is the probability that two randomly chosen letters in a block of text are identical. We know $IC_{english} \approx 0.067$, and $IC_{random} \approx 0.0385$

$$IC = \frac{1}{N(N-1)} \sum_{i=1}^{n} F_i(F_i - 1) \quad (3)$$

- N is the length of the text
- n is the length of the alphabet
- F_i is the frequency of the ith letter in the alphabet





- In the first plot, there are peaks at 5, 10, 13 and 15 alphabets. This indicates that the length of the keyword for the Vigenére deciphering is a multiple of 5. Starting with a keyword of length 10, as it has the highest peak, lead to **'PALIMPSEST'** being identified as the key word.
- Similar observations for the second plot lead to **'ABSCISSA'** eventually being identified as the keyword.

6. Transposition Cipher

- A **transposition cipher** takes the original text and creates an **anagram** of it based on a regular system or **algorithm**.
- By taking the text in the green section and reversing the order, you can use the following key, 1526374, based on the word KRYPTOS, to decipher the message.
- The key is obtained as follows:

$$\begin{array}{|c|c|}\hline K & T \\ \hline R & O \\ \hline Y & S \\ \hline P & \\ \hline \end{array} = \begin{array}{|c|c|}\hline 1 & 5 \\ \hline 2 & 6 \\ \hline 3 & 7 \\ \hline 4 & \\ \hline \end{array} = 1526374$$

(When read **horizontally***)*

- The same method of using columns containing 4 letters and 3 letters is used in the rearrangement of the green section during decryption.
- The **similarity** between generating a key, and deciphering the text leads to the belief that this may be the **intended method** of decryption by the **author**.

7. K4 Discussion

- Frequency analysis of **K4**, with comparison to the English language, shows that the use of a poly-alphabetic cipher for encryption is plausible.
- IC calculations give a flat graph with no peaks near the IC of the English language. This contradicts the point above but allows the possibility of **multiple encryption methods** being used for K4.
- Using a clue given by Jim Sanborn, the sculpture creator, that **NYPVTTMZFPK** decrypts to **BERLINCLOCK**, possible shifts for a polyalphabetic cipher are: 11, 17, 2, 5, 15, 9, 8, 7, 20, 0

8. Future work

- Research how **Hamiltonian cycles** can be used to solve a large Transposition cipher and normal anagrams.
- Research how to use a combination of a Transposition cipher and a Vigenére cipher to solve the final part of Kryptos.

References:
1. National Security Agency. 1993, June 9. CIA KRYPTOS sculpture - Challenge and resolution. United States Government - Memorandum. https://docs.google.com/file/d/0B7G1aFZQuZtXRmRkcmhkNGtqQ2c/edit.
2. Stein, D. 1999. Cracking the Courtyard Crypto. https://nsarchive2.gwu.edu//NSAEBB/NSAEBB431/docs/intell_ebb_010.PDF