Polybius Square Cipher

Polybius Square Cipher

Keane J. Moraes

History

The Polybius Square was invented by the Greeks Cleoxenus and Democleitus but was made famous by the historian and scholar Polybius, earning him a cipher named after him. This cipher was not meant as a stand-alone cipher but rather as an aid to telegraphy.

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

Modern Usage

The Polybius square cipher is not as popular as some of its variants are. One of its variants, Tap Code (a.k.a Knock Code), was used as a means of communication by US prisoners of war during the Vietnam War. They used it by tapping on the metal bars on the jail cells. In Vietnam, this tap code was very successful. Prisoners not allowed to talk would tap each others thigh.

Polybius, being a monoalphabetic substitution cipher, is vulnerable to Frequency Analysis and thus in the modern era offer no security at all.

Encryption and Decryption Algorithms

Encryption

A standard Polybius Square is a 5×5 table containing 25 characters. The English alphabet has 26 characters and as a consequence, the standard practice is to omit the letter 'J' during encryption. Instead of using a matrix in code (which would use more memory and take more time to run), we utilize some handy tools from modular arithmetic to come up with some formulas to achieve the same task. This way our code is more efficient. The method is as follows.

Given a standard Polybius Square,

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

The trick is in spotting a general formula in generating the rows and columns. Let R_i and C_i denote the row and column of the i^{th} character respectively.

$$R_i = \left\lfloor \frac{i}{5} \right\rfloor + 1$$

$$C_i = i \mod 5 + 1$$

We will perform a letter-by-letter encryption. We must take into account the conversion of the ASCII character values $\big(a(97) - z(122)\big)$ or $\big(A(65) - Z(90)\big)$ into the standard format $(0 - 25)$ else the modular arithmetic will not work with a modulo of 26.

Let E_t be the cipher text.

P_t be the plain text having length 'n'.

S be the shift, where $S \in \mathbb{N}$

$E_t = E_1E_2E_3 \dots E_n$ where E_i is the i^{th} character of the cipher text

The i^{th} character of the cipher text is computed -

If the letter is between 65 and 90 (Uppercase)

$$E_i = \Big[R_{P_i-65} || C_{P_i-65}\Big]$$

If the letter is between 97 and 122 (Lowercase)

$$E_i = \Big[R_{P_i-97} || C_{P_i-97}\Big]$$

where || stands for concatenation.

Decryption

We will perform a letter-by-letter decryption. The formulas used in the decryption algorithm are the math formula 'reversed'

Let E_t be the cipher text having length of n

P_t be the plain text

S be the shift, where $S \in \mathbb{N}$

$P_t = P_1P_2P_3 \dots P_n$ where P_i is the i^{th} character of the plain text

The i^{th} character of the plain text is -

If the letter is between 65 and 90 (Uppercase)

$$P_i = \Big[(R_i - 1) \times 5 + C_i\Big] + 65$$

If the letter is between 97 and 122 (Lowercase)

$$P_i = \Big[(R_i - 1) \times 5 + C_i\Big] + 97$$

Variants and Cryptanalysis

There are several variants of the Polybius square cipher, so much so that Polybius Square is a type of encryption scheme. The list of variants is as follows :

- Tap Code
- Bifid Cipher
- Trifid Cipher
- ADFGX Cipher
- Wheatstone-Playfair Cipher
- Nihilist Cipher