Polybius Square Cipher

Polybius Square Cipher

Keane J. Moraes

1. 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

2. 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 offers no security at all.

3. Encryption and Decryption Algorithms

3.1. 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
normASCII :	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
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 $S \in \mathbb{N}$
$E_t = E_1 E_2 E_3 \dots E_n$ 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.

3.1.1. Code Implementation

The code implementation of the encryption algorithm is a simple conversion from mathematical form to Java code. Note that we will only deal with upper case letters in the code implementation. The reader is free the lower case version.

```
42  for (int i = 0; i < plainText.length(); i++) {
43    int letterNumber;
44    if ((plainText.charAt(i) < 65 || plainText.charAt(i) > 90)
45    && (plainText.charAt(i) < 97 || plainText.charAt(i) > 122)) {
46      result = result.concat(plainText.charAt(i) + "");
47      continue;
48    } // if statement - special characters
```

First as always we take care of the the special characters. Anything not in the $[65, 90]$ range gets tacked onto the result.

```
59    if (plainText.charAt(i) >= 'J')
60      letterNumber = plainText.charAt(i) - 66;
```

Here comes the tricky part. Recall that our mathemtical formula for encryption we omitted the 'J'. So the alphabet numbering would be $I - (9),\ K - (10)$. The reason we subtract by 66 is so that K and all the letters after it will map to 10 and all the numbers after it. K's ASCII is 76 so subtraction by will result in a 'normASCII' value of 10 which is what we want.

```
61        else
62      letterNumber = plainText.charAt(i) - 65;
```

If the letter is not above 'J' then we proceed normally and subtract by 65.

```
63        int rowNumber = (int)(Math.floor(letterNumber / 5) + 1);
64        int columnNumber = letterNumber % 5 + 1;
65        result += (rowNumber + "") + (columnNumber + "") + " ";
```

Here we implement the formulae discussed earlier. Notice that we need to explicitly typecast the `rowNumber` since `Math.floor` returns a float. The concatenation of the two is added onto `result`.

3.2. 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)

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

3.2.1. Code Implementation

The code implementation of decryption is also a translation of formulae into code.

```
81  for (int i = 0; i < encryptedText.length(); i += 3) {
82    int letterNumber = Integer.parseInt(encryptedText.substring(i, i + 2));
```

The `for`-loop jumps 3 because it has to go from coordinate to coordinate each of which are 3 characters apart. For example, to get from the first coordinate pair to the second coordinate pair, you have to increment by 3.

$$\overset{i}{45}\ \ 31$$

```
84    if (letterNumber / 10 > 2 || (letterNumber / 10 == 2 && letterNumber % 10 == 5))
85      letter = (char) (65 + (letterNumber / 10 - 1) * 5 + (letterNumber % 10));
86        else
87      letter = (char) (65 + (letterNumber / 10 - 1) * 5 + (letterNumber % 10 - 1));
88    result += letter;
```

The `if` statement formula essentially asks

- Is the row numbers greater than 2? (or)

- If the row number is 2, then is the column number equal to 5?

Why do we need to do this? Because we have to omit mapping J. Every letter after 'J' in the ASCII table will have this correctional measure hence the nature of the `if`-statement. Recall that to map from rows and columns to ASCII we have to multiply the row by 5 and add the column and then add 65. Take for example K. It has a square coordinate of 25 meaning that it will map to $65 + (5 \times (2 - 1) + 5) = 75$ which is the result we wanted since 75 is the ASCII for 'K'. If this correctional measure was not in place then we would get $65 + (5 \times (2 - 1) + (5 - 1)) = 74$ which is the ASCII value of 'J'.
However, for any element before 'J' this correctional formula doesn't apply. Take for example G. The square coordinate for G is 22. This maps to $65 + (5 \times (2 - 1) + (2 - 1)) = 71$ which is correct ASCII table value of G.
The result of this is then attached to `result`.

4. Variants

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 :

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

We will discuss only the Tap Code, ADFGX and Nihilist here. Bifid, Trifid and Wheatstone-Playfair are complex enough to get their own code and documentations.

4.1. Tap Code

Tap Code also known as Knock Code is a simple modification to the Polybius Square cipher. Instead of numbers to represent the row and column coordinates, dots are used. This was used by Russian prisons of the czar and American prisoners in Vietnam to communicate between each other. They used it to communicate everything from what questions interrogators were asking (in order for everyone to stay consistent with a deceptive story), to who was hurt and needed others to donate meager food rations.

4.2. ADFGX Cipher

The ADFGX cipher is a simple modification of the Polybius cipher. Instead of using numbers (1-5) for rows and columns, it uses the letters A,D,F,G and X. It was invented by the German intelligence officer Fritz Nebel and first used in March 1918. These letters were chosen as such since they are very different from each other in Morse Code thus minimizing the possibility of operator error. [1]

[1] Read more about the ADFGX cipher on its Wikipedia page

4.3. Nihilist Cipher

The Nihilist cipher was a symmetric key variant of the Polybius square used by the Russian nihilists to plan terrorist attacks against the tsarist regime in imperial Russia. The square coordinates of the key and the plaintext would be added to get the resultant cipher text. So for example if I had the plaintext "IWANTHIMDEAD" with a key "ALCAPONE" then we would get

PT : 24 52 11 33 44 23 24 32 14 15 11 14

KY : 11 31 13 11 35 34 33 15 11 31 13 11

CT : 35 83 24 44 79 57 57 46 25 46 24 25

This essentially makes it a numerical version of the Vignère cipher. There is no fractionation achieved. Hence a modified Kasiski examination will work on cracking this cipher.[2]

5. Further Reading

Fractionating Ciphers

Read more about Fractionating ciphers on Crypto Corner

Read the Bifid and Trifid documentation to learn more about fractionation.

[2]To read about an upgraded model of the Nihilist cipher (which implements fractionation), refer to the Bifid cipher.