

Names: Yasar Azimi

ID:# 44158

Assignment 2

Dr.Abdalrahman Alfagi

Class: ITC 370

2023/11/20

Introduction:

In cryptography, classical encryption methods have played a pivotal role in securing information. This report explores and explains five classical ciphers which includes: Hill Cipher, Reverse Order, Geometric Cipher, Rail Fence Cipher, and Double Transposition Cipher. Each cipher has its unique approach to encrypting messages, providing insights into historical cryptographic techniques.

Main Body:

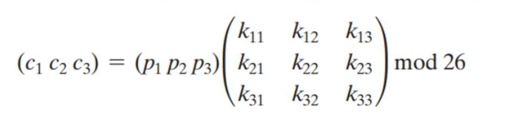
**1. Hill Cipher:**

The Hill Cipher, invented by the mathematician named Lester Hill in 1929, is a multi-letter cipher and the first polygraphic substitution cipher. It is capable of encrypting groups of letters, di-graphs, tri-graphs, or poly-graphs at a time, making it more complex than other ciphers studied thus far. The cipher is based on linear algebra and utilizes matrix mathematics, so having a good background in linear algebra and matrix mathematics is necessary to truly understand the workings of hill cipher.

1. **Hill Cipher Encryption:**

To encrypt a text using the Hill cipher, we can follow the procedures bellow:

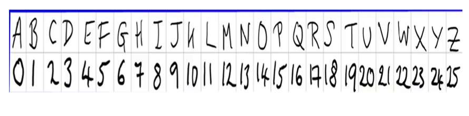
1. Select the plaintext.
2. Select a key matrix (whether it’s 3x3 or 2x2).
3. Divide the message into blocks of letters, where the number of letters in each block is equal to the dimension of the key matrix. Meaning if the key is 3x3 then we select the words in groups of 3 otherwise if the key is 2x2 then we select the words in group of 2.
4. Represent each block as a vector, with each letter assigned a numerical value from 0 to 25.
5. Multiply each block vector by the key matrix, modulo 26.



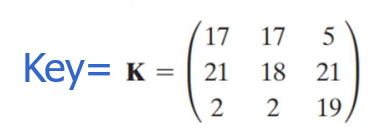
1. The encrypted message is the sequence of letters corresponding to the encrypted vectors.

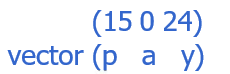
Example:

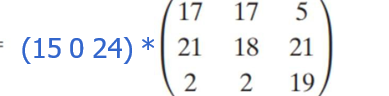


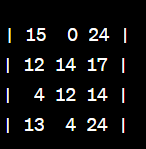


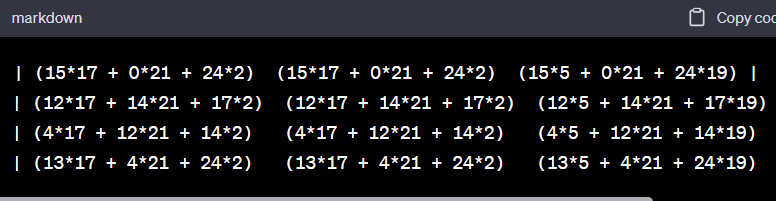


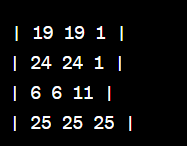


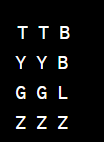
 











**The answer comes to: TTBYYBGGZZZ**

1. **Reverse Order Cipher**

The simplest implementation of a transposition cipher is to reverse the plain text. Now the Reverse Order Cipher involves reversing the order of characters in the plaintext either with a selected key pattern or without one by just reversing its form, and the process of encryption and decryption is the same, just in reverse.

Example:

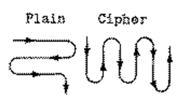
1. If the plaintext is "HELLO," the cipher-text is "OLLEH."
2. If plain text is “Price of blood ” the cipher text is “doolb fo ecirp”
3. **Geometric Cipher**

The Geometric Cipher arranges plaintext in a specific geometric shape and reads it off in a different order. The step needed for geometric cipher include:

1. A geometric shape is chosen.
2. Plaintext is written in the shape.
3. Cipher text is read off in a different order.

Example:

1. If we choose a key-pattern for cipher-text,



Now if plain text is “Prince of Persia” we write it as:

P r i n c e o

F p e r s i a

For the cipher text we get:

**Cipher** = pfrp ienr csei oa

1. **Rail-Fence Cipher**

The Rail-Fence Cipher is a transposition cipher that writes plaintext in a zigzag pattern and reads off the cipher text. So basically the plain text is written down-wards/in a zigzag pattern, and you start a new column when the end is reached while the cipher text is read off from the pattern we used.

To do this we use the following steps.

1. We choose a plain text.
2. We choose a pattern.
3. We put the plain text (alphabet by alphabet) in the said pattern.
4. Then we read it as row by row.

**Example:**

Plain text = we have a good weather today.

W h v a o d e t e t d y

E a e g o w a h r o a

Cipher text = whvaodetetdyeaegowahroa

1. **Double transposition Cipher**

Double transposition cipher is one of the most secure hand written method of cipher used in the Second World War. As for its process it applies two consecutive columnar transposition to a messages. The key can be either the same or different for both of the processes.

* Plaintext = your mother was a hamster and your father smelt of elderberries
* Key= Describe



**Cipher** = yemyefrorsoreruwtusliraermdemsrfeesoaaalrthnttbhadhoe

**Conclusion:**

In conclusion, we can say that classical encryption techniques offers a diverse methods for securing information. The Hill Cipher, leveraging linear algebra, provides robust encryption, while simpler methods like Reverse Order and Rail Fence Cipher offer quick solutions. Geometric Cipher introduces a creative approach, and Double Transposition Cipher combines transposition for added complexity. Understanding these classical ciphers aids in appreciating the evolution of encryption and choosing appropriate methods for different security requirements. As we delve into more advanced cryptographic techniques, these classical ciphers remain foundational in understanding the principles of secure communication.