Encryption and Decryption

MAT 248: Applied Linear Algebra-Section II

Group 15: Triple Threat

Anshi Shah: AU2040087

Varun Parekh: AU2040011

Vanshit Shah: AU2040098

***Abstract*—Data security, encompassing confidentiality, access control, integrity, and availability, has been a major challenge in data communication from the dawn of time. This is essentially the goal of cryptography: to investigate methods for securing sensitive communications through information encryption and decryption. Several methods have been developed that have helped to build the foundations of existing cryptographic algorithms. Hill Cipher devised several primary methods in classical cryptography, involving a variety of mathematical techniques. Hill Cipher, despite modern advancements, provides a simple and unique means to hide messages in plain sight.**

***Keywords*—Hill Cipher, encryption, decryption, cryptography, matrices**

I. Introduction

Authentication of information has become a fundamental part of our lives as privacy. People have attempted to share the information anonymously since the development of the composed language. Encryption and decryption of information using various cryptographic methods play a crucial role in the world to authenticate personal or organizational data. Cryptography provides several mechanisms for such techniques. One such method is Hill Cipher. This cryptographic technique was developed in attempt to build an encryption that could not be cracked using frequency analysis. The Hill Cipher is a polygraphic substitution cipher based on Linear Algebra principles. Modulo arithmetic, matrix multiplication, and matrix inverses are all the concepts used in the Hill cipher technique.

II. Background

Information security has been a significant challenge in data transmission since the dawn of humanity. It must have been prominent in the sender's mind when a sensitive message was etched on a clay tablet or painted on the royal walls that the information not be intercepted and read by a rival. As a result, codes are a significant part of our past; from Da Vinci's and Michelangelo's paintings to ancient Roman steganographic practices, the need for data hiding was clear.

III. Motivation

The need to secure communications from prying eyes is greater than ever before in this era of internet. Cryptography, or the study of encryption, is used in many parts of daily life, including mobile phone communication, e-commerce, sending private e-mails, and conveying financial information. Today's technology may

be traced back to the earliest ciphers and has evolved over time. As the early cyphers were cracked, new, more powerful ciphers emerged.

In cryptography, the Hill Cipher is a technique used to describe how to employ matrices defined over a finite field and how to handle characters and strings in computer applications. One of the symmetric key techniques with various advantages in data encryption is the Hill Cipher algorithm with self-repetitive matrix. In comparison to other strategies such as the self-invertible matrix, this method is simpler to implement.

IV. Literature Survey

This project demonstrates how encryption and decryption textual data works using the Hill Cipher algorithm. In cryptography, the Hill Cipher was one of the first polygraphic cipher systems based on a workable system with more than three symbols or letters in one. Hill cipher is a block cipher with various advantages, including hiding plaintext letter frequencies, being simple to encrypt and decrypt due to the use of matrix multiplication and inversion, and having a high speed and efficiency.

In this project, there is also provided an advanced Hill Cipher method that encrypts data using an involutory key matrix. The goal of this study is to solve the disadvantage of utilizing a random key matrix in the Hill cypher technique for encryption, which is that if the key matrix is not invertible, we may not be able to decrypt the encrypted data. Because we employ an involutory key matrix for encryption, we can also further reduce the computational complexity by skipping the process of determining the inverse of the matrix during decryption.

Hill Cipher encryption is a clever use of matrices, but soldiers in the trenches watching artillery shells pass overhead are unlikely to be able to perform matrix multiplication. Hill Cipher is more difficult to use and weaker than the Playfair cypher for encrypting digraphs.

The Hill system's ponderousness is, of course, the fundamental barrier to its practical application. Hill attempted to mitigate this by inventing a gadget that can decode tiny Polygram. Upskilling to emerging technologies has become the need of the hour, with technological changes shaping the career landscape.

Therefore, we would like to go into in-depth research for Hill Cipher to know more about its use and invention.

V. Mathematical Model

A. *Text Encryption using Hill Cipher*

Text encryption is a process of converting a normal text message, also known as Plain text into a completely meaningless text, also called Cipher text. This is done using the Hill Cipher method developed by Lester Hill.

The formula used for encryption is given as:
Cipher Text = (Plain Text * Key) Mod 26

The algorithm:
Step 1: Each letter in the alphabet is assigned a number from 0 to 25 from a to z such that a = 0, b = 1, …, z = 25.

Step 2: The Plain text or the message that is inputted is then converted into a *n x 1* matrix. For example, the string ‘ACT’ would be converted to a *3 x 1* matrix as shown:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

Step 3: The key string is entered and the *n x 1* matrix is then converted to a *n x n* matrix. Here, n is the length of the string entered.
For the above example, we take the key as ‘GYBNQKURP.’

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Step 4: As per the above-mentioned formula, the *n x n* matrix (key matrix) is multiplied to *n x 1* matrix (plain text matrix) to get the ciphered vector.

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix}$$

Step 5: The ciphered vector is then converted to Mod 26.

$$\begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

Step 6: In the final step, the vector is converted back to letters and we get the encrypted text as the result. Here, converted string is ‘POH.’

B. *Text Decryption Using Hill Cipher*

Decryption means getting back the original message from the encrypted message. Decoding the message includes taking inverse of the key matrix that was used for encryption.

The formula used for decryption is given as:
Plain Text = (Cipher Text * Key $^{-1}$***) Mod 26***

The algorithm:
Step 1: The ciphered text that we get as a result of encryption is inputted. It is converted into a *n x 1* matrix. In the above example, ‘POH’ was the encrypted text. The *n x 1* matrix made is,

$$\begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

Step 2: Enter the key used for encryption, and it gets converted into a *n x n* matrix again. They key used was 'GYBNQKURP.'

Step 3: According to the formula for decryption the inverse of the key matrix is calculated and then it is multiplied to the cipher text matrix to get the plain text matrix.

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

Step 4: The plain text matrix then generated is again converted to Mod 26 to get back the original *n x 1* matrix.

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

Step 5: The numbers in the matrix are converted back to letters and thus the text gets decrypted, returning the original message back.

C. *Linear Algebra Concepts Used In Hill Cipher*

1. Matrix Multiplication
2. Determinant of a Matrix
3. Inverse of a matrix
4. Modular Multiplicative Inverse

D. *Code Implementation*

Python language is used for the coding implementation. Following libraries and functions are used:

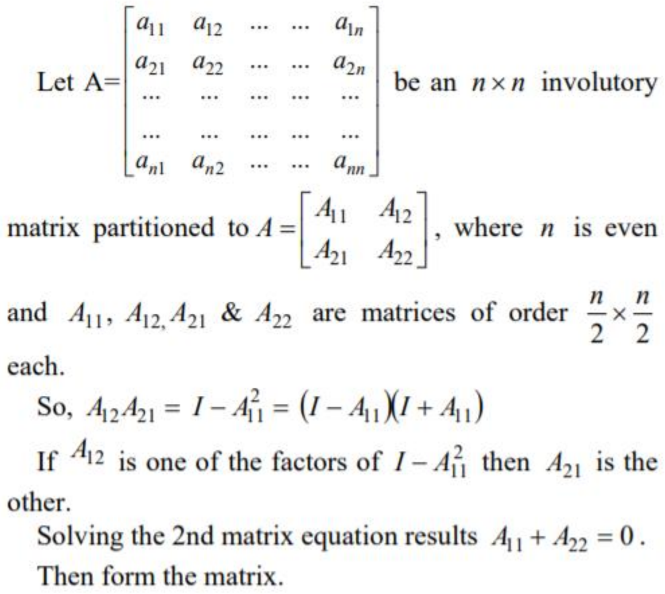
1. init() function
2. ord() function
3. Numpy library for matrix declaration and manipulation
4. Sympy for matrix manipulation
5. Colorama library for user interface
6. Termcolor library for user interface

E. *Image Encryption & Decryption Using AdvHill*

The Advanced Hill Cipher method is a modified version of the Hill Cipher method used in image cryptography. For encryption, this method employs an involuntary Key Matrix. We additionally utilise mod 256 to determine the colour composition of the image instead of the basic equation Cipher image = Key.Pixel. For grey scale photos, the algorithm will be utilised directly. If the image is coloured, the R-G-B (Red, Green, Blue) components should all be worked on separately using the same approach. After that, the individual elements can be concatenated.

- *Generation of Involuntary Matrix*

A is called an involutory matrix if $A = A^{-1}$. The analysis presented here for generation of involutory key matrix is valid for matrix of positive integers that are the residues of modulo arithmetic of a number. This algorithm can generate involutory matrices of order $n \times n$ where n is even.



Let A= $\begin{bmatrix} a_{11} & a_{12} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & \cdots & a_{nn} \end{bmatrix}$ be an $n \times n$ involutory matrix partitioned to $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$, where n is even and A_{11}, $A_{12,}A_{21}$ & A_{22} are matrices of order $\frac{n}{2} \times \frac{n}{2}$ each.

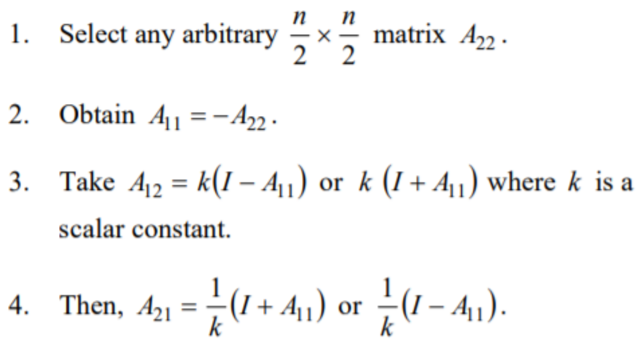
So, $A_{12}A_{21} = I - A_{11}^2 = (I - A_{11})(I + A_{11})$

If A_{12} is one of the factors of $I - A_{11}^2$ then A_{21} is the other.

Solving the 2nd matrix equation results $A_{11} + A_{22} = 0$.

Then form the matrix.

The algorithm:



1. Select any arbitrary $\frac{n}{2} \times \frac{n}{2}$ matrix A_{22}.
2. Obtain $A_{11} = -A_{22}$.
3. Take $A_{12} = k(I - A_{11})$ or $k\ (I + A_{11})$ where k is a scalar constant.
4. Then, $A_{21} = \frac{1}{k}(I + A_{11})$ or $\frac{1}{k}(I - A_{11})$.

- *Image Encryption Algorithm*

Step 1: A involutory key matrix of dimensions *m* × *m* is constructed.

Step 2: The plain image is divided into m× m symmetric blocks.

Step 3: The ith pixels of each block are brought together to form a temporary block. Hill cipher technique is applied onto the temporary block. The resultant matrix is transposed and Hill cipher is again applied to this matrix.

Step 4: The final matrix obtained is placed in the ith block of the encrypted image.

- *Image Decryption Algorithm*

Step 1: Take the matrix formed by dividing the encrypted image into m blocks.

Step 2: From each such block, the it^{h} pixel is brought together to form a block (P).

Step 3: Apply Hill Cipher formula using inverse of the same key as encryption
(P = K^{-1}. C mod 256) (Here the same matrix since it is the inverse of itself)

Step 4: The resultant matrix is transposed and Hill Cipher is again applied.

Step 5: The matrix thus obtained forms the ith block of the original meaningful image.

F. Linear Algebra Concepts Used

1. Matrix multiplication and manipulation
2. Involuntary Matrix Generation
3. Modular Arithmetic

G. Code Implementation

Python language is used for the coding implementation. Following libraries and functions are used:

1. Imageio for handling and reading images

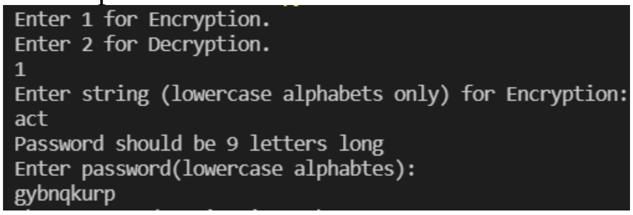
2. Concatenate function - This function is used to join two matrices. In the case of a matrix corresponding to an image, it is 2D if the image is grayscale and 3D if the image is coloured.
3. numpy.resize

VI.

VII. Numerical Results

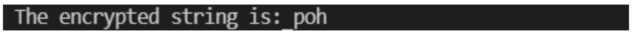
A. *Results of Text Encryption*

User Input:



```
Enter 1 for Encryption.
Enter 2 for Decryption.
1
Enter string (lowercase alphabets only) for Encryption:
act
Password should be 9 letters long
Enter password(lowercase alphabtes):
gybnqkurp
```

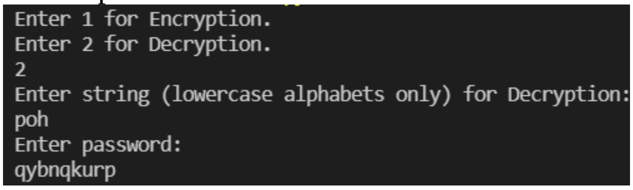
Output:



```
The encrypted string is: poh
```

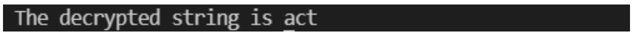
B. *Results of Text Decryption*

User Input:



```
Enter 1 for Encryption.
Enter 2 for Decryption.
2
Enter string (lowercase alphabets only) for Decryption:
poh
Enter password:
qybnqkurp
```

Output:



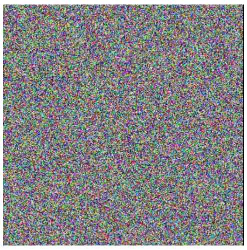
```
The decrypted string is act
```

C. *Results of Image Encryption*

User Input:

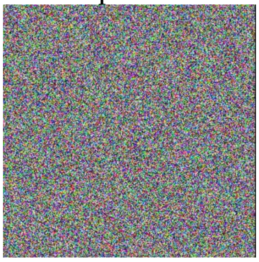
Output:

Encrypted image is generated.



D. *Results of Image Decryption*

User Input:



Output:

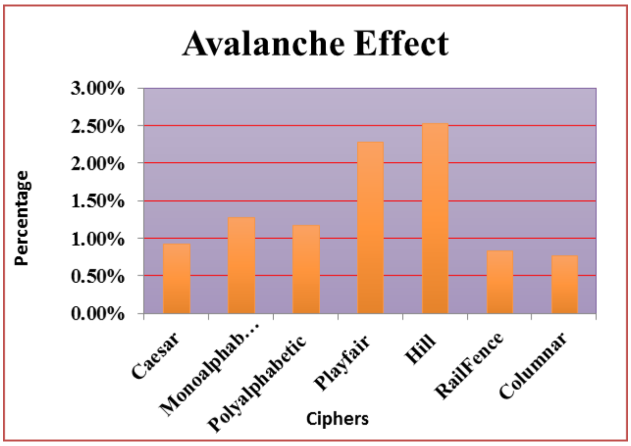
Decrypted Image is generated.

E. *Observations and Inferences*

➢ *The Avalanche Effect:*

In cryptography the avalanche effect is associated with the behaviour of mathematical functions used for encryption. It is one of the desirable properties for any encryption algorithm. A slight change in the key or the plain text results in a significant change in the cipher text. In other words, it quantifies the effect on the encrypted text even for a small change in the key.

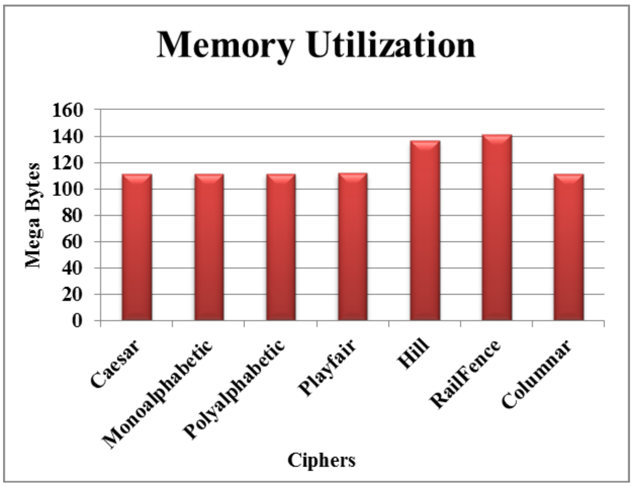
Following is the comparison of Avalanche effect of Hill Cipher with other techniques.



- *Memory Utilization:*

Different encryption algorithms necessitate different memory sizes to be implemented. The amount of memory required is determined by the number of operations to be performed with the method, the key length utilized, the initialization vectors used, and the type of operations. The amount of memory used has an impact on the device's price. It is preferable that the amount of recollection required be kept to a minimum.

Following is the comparison of memory utilization of Hill Cipher with other techniques.



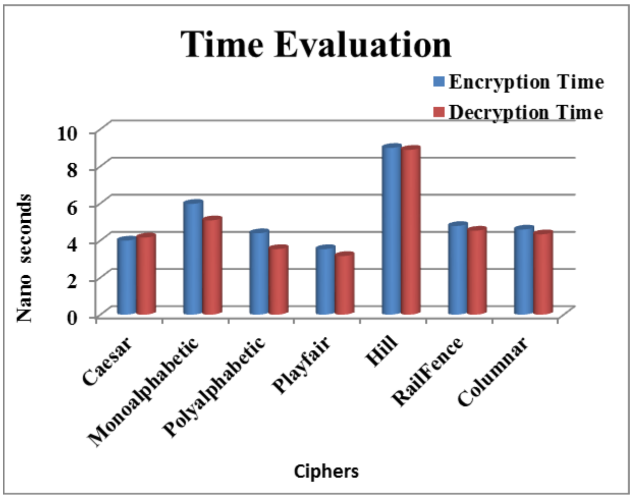
[Image]

- *Time Evaluation:*

Encryption and decryption durations are used to calculate time. The time it takes to encrypt plaintext is known as encryption time.

The amount of time it takes to encrypt data has an impact on the procedure's overall execution. The length of the plaintext, key size, algorithm complexity, and processor speed all affect encryption time. Encryption time must be significantly reduced in order for the device to be speedy and responsive.

The time it takes to decrypt cipher text into readable plaintext is called decryption time. To keep things quick and responsive, the decryption time should be substantially shorter than the encryption time. The time it takes to encrypt and decrypt data is measured in nanoseconds.



VIII. Contributions

Anshi: Research, Algorithm for images encryption, Coding, Report, Ppt

Varun: Research, Hill Cipher Observations, Algorithms, Coding, Report, Ppt

Vanshit: Reseach, Algorithm for texts, Coding, Ppt, Report

IX. References

[1] Acharya, Bibhudendra & Panigrahy, Saroj Kumar & Patra, Sarat & Panda, Ganapati.

(2009). Image Encryption Using Advanced Hill Cipher Algorithm. International Journal of Recent Trends in Engineering. 1. https://www.researchgate.net/publication/229012891_Image_Encryption_Using_Advanced_Hill_Cipher_Algorithm

[2] Donni Lesmana Siahaan, Muhammad & Siahaan, Andysah Putera Utama. (2018). Application of Hill Cipher Algorithm in Securing Text Messages. https://www.researchgate.net/publication/328693056_Application_of_Hill_Cipher_Algorithm_in_Securing_Text_Messages

[3] S. Kingslin and R. Saranya, Analysis of Avalanche effect. 2018.

[4] Prerna, Urooj, M. kumari, and J. N. shrivastava, “Image Encryption and Decryption using Modified Hill Cipher 26 Technique,” International Journal of Information & Computation Technology, vol. 4, no. 17, pp. 1–8, 2014.