IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

The Hill Cipher Algorithm for Data Encryption and Decryption

Ayush Gupta
Student, Department of Computer Science & Information Technology
Dronacharya College of Engineering, Gurugram, India

Abstract: *The science of encoding and decoding signals is known as cryptography. Cryptography is frequently used in people's daily life to keep sensitive data, such as Mastercard data, safe. Many regular exercises can be easily viewed by unintentional outsiders via the Internet. Hill cipher is a simple linear transformation represented by a matrix that is a traditional cryptography based on linear algebra. It is one of the symmetric key algorithms with various data encryption advantages. However, the inverse of the plaintext encryption key matrix is not always available. The encrypted text cannot be decoded if the key matrix is not invertible. The key matrix employed for encryption in the Involutory matrix generation method is invertible. As a result, we do not need to find the inverse of the key matrix during decryption.*

Keywords: Symmetric Key Algorithms

I. INTRODUCTION

Third parties or organisations cannot access sensitive information thanks to cryptography, which is the study and practise of secure communication using unique methods and procedures. Confidentiality, data integrity, authentication, and other notions are critical in modern cryptography.

Lester S. Hill, a distinguished American mathematician, conceived and developed the Hill Cipher method in 1929. Hill Cipher employs a variety of mathematical techniques, including numerous traditional cryptographic approaches. Plaintext is separated into groups of letters of a predetermined size, and each group is turned into a different group of letters by the Hill cipher. Matrix multiplication, which is used in both encoding and decoding, is used to achieve this transformation. Every second, a vast amount of data is carried over the Internet, and one sort of data, that which employs matrix to encode a message, is particularly tough to crack. The encoding matrix is the initial matrix of Hill cipher, and its inverse is the decoding matrix. This self-repetitive Hill Cipher technique first determines whether or not the matrix used to encrypt the plaintext is invertible. If the encryption matrix isn't invertible, the algorithm changes it so that the inverse may be found.

II. MAJOR IDENTIFICATION

Data security, including confidentiality, access control, integrity, and availability, has long been a fundamental concern in data communication. It must have been forefront 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. When this competitor obtains data that cannot be encrypted using a different cryptographic technique, the data may be altered or corrupted by various denial of service attacks on the communication channel.

The Hill Cipher algorithm for data encryption and decoding has various flaws. The first is that because this approach uses very weak symmetric key methods, it is easy to cryptanalyze by competitors. The second data encrypted by this method sometimes cannot decrypt to the original plaintext. Because the encrypted text cannot be deciphered, the third problem with Hill Cipher is that there are no invertible matrices. Two plaintext vectors will be mapped into the same cipher text vector if the matrix is not invertible. As a result, the proposed methods used Hill cipher with self-repetitive matrix to encrypt and decode data back to its original plaintext.

2.1 Hill Cipher Algorithm

The Hill cipher is a polygraphic substitution cipher based on Linear Algebra principles. The Hill cipher is more mathematical than others since it uses modulo arithmetic, matrix multiplication, and matrix inverses. Because the Hill cipher is also a block cipher, it can theoretically function with blocks of any size. While Hill Cipher is digraphic in nature,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

it may be expanded to multiple any size of letters for added complexity and reliability. Because the majority of Hill Cipher issues and solutions are mathematical in nature, concealing letters with precision becomes simple.Each block of n letters (seen as an n-component vector) is multiplied by an invertible nxn matrix against modulus 26 to encrypt a message. Each block is multiplied by the inverse of the matrix used for encryption to decrypt the message.The cipher key is the encryption matrix, and it should be chosen at random from the set of invertible nxn matrices (modulo 26).

2.2 Encryption

Each letter is first encoded as a number. The most common scheme used to be: A = 0, B = 1, …, Z =25 Then, the message that is to be encrypted will be held in a block of n letters considered as a vector of n dimensions. It will then be multiplied by an n x n matrix known as the key matrix. Then the result will be converted with modulo 26 (in this case, since the alphabet has 26 letters). This will yield the cipher text.

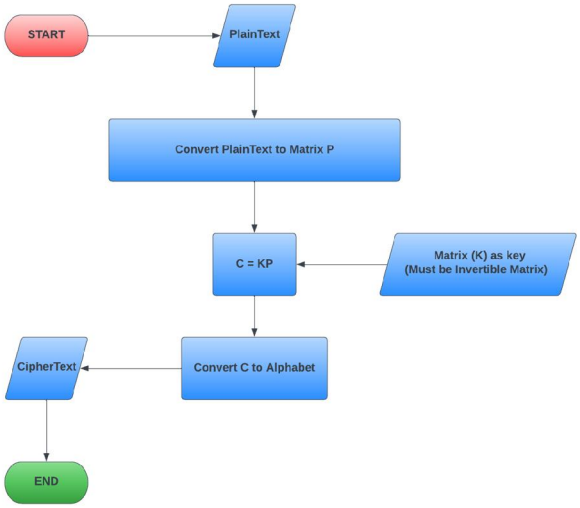

Fig. 1.

Hill Cipher's encryption technique is described in above flowchart. The plaintext to be encoded is the first step in this procedure. The plaintext is then transformed using certain criteria into a matrix form (P). As the encryption key, the matrix (P) will be multiplied by the matrix (K). Because the matrix (K1) will be the key in the decryption procedure, it must be invertible. The result of multiplying the matrices (P) and (K) will be a matrix (C). The same rules that were used to transform the plaintext into a matrix are used to convert this matrix into alphabetical form.

2.3 Mathematical Process

Given the plain text message: “paymoremoney”

Encoding to the message to numbers yields:

P = 15, 0, 24, 12, 14, 17, 4, 12, 14, 13, 4, 24

Then for example using the key:

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

We’ll want to get the cipher text which the formula is:

C = PK mod 26

Then since the key is a 3×3 matrix, then we can use the first three letters of the message and multiply them by the key matrix like so:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

$$C = (15, 0, 24)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

= (303, 303, 531) mod 26

= (17, 17, 11) = RRL

Repeating this process with obtain that the encrypted string is:

C = RRLMWBKASPDH or in numbers C = 17, 17, 11, 12, 22, 1 ,10, 0, 18, 15, 3, 7

2.4 Decryption

To decrypt, we store the encrypted text in an n-dimensional vector, just like the plain text. Then we multiply by the key matrix's inverse. In actuality, this isn't a typical inverse matrix. It is highly reliant on the modulo employed. The generated matrix will then be modulo 26 converted. This returns the original message.

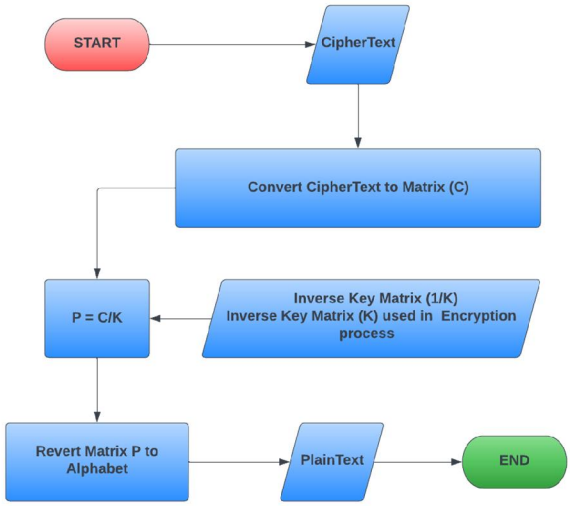

Fig. 2.

The decryption procedure in Hill Cipher begins with the Ciphertext as input, as shown in the diagram above. With certain rules, this Ciphertext will be translated into a matrix form (C). The inverse of the key matrix used during encryption will be multiplied by the matrix (C) to obtain a matrix (P). The decryption process is completed by converting the matrix (P) back to alphabetical form using the same principles that were used to convert Ciphertext to matrix form.

2.5 Mathematical Process

Given the cipher text in numerical value:

C = 17, 17, 11, 12, 22, 1 ,10, 0, 18, 15, 3, 7

We want to obtain the plain text which is:

P = C / K mod 26

But we need to get the inverse of the key matrix. This process has some differences to the normal means of getting a matrix inverse. With the key we do the adjoint of each element and then transpose it and we obtain:

$$\begin{pmatrix} -300 & 313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{pmatrix}$$

Now what is different is the way the determinant is computed, we have that normally our determinant would be:

detK = -939

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

But the Hill Cipher uses a modulo so the real determinant would have to be converted with modulo 26, to obtain its correct values, hence we have:

-939 mod 26 = -939 – 26 x floor(-939 / 26)

= 23

Then the multiplicative inverse of the determinant must be computed which yields:

(1 / 23) mod 26 = 17

Because the modulo of the product between the determinant and the multiplicative inverse yields 1

(23 x 17) mod 26 = 1

Then we multiply the adjoint matrix by the multiplicative inverse with the modulo and we obtain the inverse of the key matrix:

$$\textbf{1 / K = 17} \begin{pmatrix} -300 & 313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{pmatrix} \textbf{ mod 26}$$

$$\textbf{1 / K =} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

And now is just a simple mean of multiplying the cipher text vectors with the inverse key matrix.

$$\textbf{P = (17 17 11)} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \textbf{ mod 26 = (15 0 24)}$$

(15 0 24) = P A Y

Which ends up giving us our original message “paymoremoney”.

III. CONCLUSION

Hill Encryption was one of the first polygraphic cipher systems to be based on a workable system with more than three symbols or letters in a single symbol or letter. Hill Cipher is rarely or never used in the present period. However, its existence in the cryptography learning curve is indisputable.

Understanding the use of Hill Ciphers in general requires both encryption and decryption. It is critical to recognise that any potential matrix in the system is not a key matrix. Instead, cipher decryption necessitates the use of an inverse key matrix.

The determinant method can tell you whether or not the inverse exists. If the determinant has a value of 0 or shares a factor other than 1, the matrix does not have an inverse. As a result, decryption will require the use of a new key matrix. To extract results from a cipher, an useable or key matrix with non-zero determinants must have a coprime component directly proportional to the overall length of the alphabet.

REFERENCES

[1]. H. Ming dan S. LiZhong, “A New System Design of Network Invasion Forensics,” in 2009 Second International Conference on Computer and Electrical Engineering, 2009, hal. 596–599.

[2]. A. Lubis dan A. P. U. Siahaan, “Network Forensic Application in General Cases,” IOSR J. Comput. Eng., vol. 18, no. 6, hal. 41–44, 2016.

[3]. F. H. Khan, R. Shams, F. Qazi, dan D.-E.-S. Agha, “Hill Cipher Key Generation Algorithm by using Orthogonal Matrix,” Int. J. Innov. Sci. Mod. Eng., vol. 3, no. 3, hal. 5–7, 2015.

[4]. A. P. U. Siahaan, “Three-Pass Protocol Concept in Hill Cipher Encryption Technique,” Int. J. Sci. Res., vol. 5, no. 7, hal. 1149–1152, 2016.

[5]. W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed. Prentice Hall, 2005.

[6]. A. P. U. Siahaan, How to Code: Advanced Encryption Standard in C#. Medan: Fakultas Ekonomi Universitas

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

Panca Budi, 2018.

[7]. A. Putera Utama Siahaan, E. Elviwani, dan B. Oktaviana, "Comparative Analysis of RSA and ElGamal Cryptographic Public-key Algorithms," in Proceedings of the Joint Workshop KO2PI and The 1st International Conference on Advance & Scientific Innovation, 2018.

[8]. X. Liu, Z. Wei, and C. J. Carter, A novel image encryption approach using block based transformation and random phase encoding,.

[9]. S. Muttoo, D. Aggarwal, and B. Ahuja, "A Secure Image Encryption Algorithm Based on Hill Cipher System," Bulletin of Electrical Engineering and Informatics, vol. 1, no. 1, 2012.

[10]. M. A. Aljanabi, N. A. Shnain, and S. F. Lu, "An image similarity measure based on joint histogram — Entropy for face recognition," in Proceedings of the 3rd IEEE International Conference on Computer and Communications (ICCC '17), pp. 1626–1631, Chengdu, December 2017.

[11]. B.M.Verdiana, Coverage 6, 2020, Retrieved from liputan6.com: https://www.liputan6.com/global/read/4214488/who-unjukkan-corona-covid-19-tak-menular-kapalair-ini-pelaksanaannya

[12]. H. Anton, C. Rorres, Elementary Linear Algebra, America, Wiley, 2004

[13]. Melvin Steven Hernández, Dr. Alfredo Cruz (Advisor, Study of the Hill Cipher Encryption/Decryption Algorithm, 28-08-2012