JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p. 194-198
https://publishoa.com
ISSN: 1309-3452

A Neoteric Strategy of Hill Cipher for Analysis of Degenerate Matrices Key

Sachin Jain[1]
Assistant Professor
Sachool of Computer & Systems Sciences
Jaipur National University, Jaipur

Ms. Khushboo Arya[2]
M.Tech Scholar
Sachool of Computer & Systems Sciences
Jaipur National University, Jaipur

Received 2022 March 15; **Revised** 2022 April 20; **Accepted** 2022 May 10.

Abstract— The Hill cipher is the principal tester encryption which has certain benefits in secure key encryption. Still, it is unresisting to recognized readable text spasms. An alternative setback is that an unavoidable key matrix is required for decryption and it is not seemly for encrypting a plaintext comprising of nil. The objective of this work is to amend the present Hill cipher to overwhelm these problems. Analysis of earlier outcomes showed that the prevailing Hill algorithms are not yet satisfactory. Specific of these algorithms are quite vulnerable to recognized plaintext. On the added, specific of these algorithms have enhanced alteration attributes and as a result, they are more resistant compared to recognized plaintext attacks.

However, these improved Hill cipher algorithms have the degenerate matrices key problem. Additionally, these algorithms are not suitable for entirely zeroes readable block encryption. In this paper, a Neoteric Strategy of Hill Cipher is proposed which applies to the invertible key matrix. Exploration of the projected algorithm is carried out via non-invertible key matrix approaches that are comparative different to understand. Preceding exploration focused on hill cipher using symmetric/asymmetric key algorithm. When the user encodes the plain text message using the hill cipher technique then the user can do, but when a user decodes the ciphertext message then some vulnerability arises. This analysis put forward to usage the hill cipher act in qualitative approach in evaluating the different vulnerabilities as an inversion of key matrix. In this exploration, a user has no trouble identifying the inversion of the key matrix when a key matrix is invertible for decryption. In previous work, there is a crisis to generate the inverse key matrix when the matrix is non-invertible because when the matrix is non-invertible means it's determinative is zero and in hill cipher determinative shows a vital role in decode. Then when it is zero then how a user can decrypt the message.

Keywords— Hill cipher, Encryption, Decryption, Symmetric /Asymmetric, Vulnerability, Non-invertible, Invertible.

1 INTRODUCTION

Today, information is one of the most valuable insubstantial assets. Due to this fact, data and information security have become an important issue. Cryptography is one of the methods to ensure the confidentiality and integrity of information. It is beginning with the Greek word “kryptos” which means secreted. Cryptography is the art and science of making a message unintelligible. It serves as a secret communication mechanism and can be traced back to thousands of years ago. Caesar’s cipher is one of the earliest known cryptosystems which was used by Julius. All of these encryptions are the underpinning for modern cryptography.

There are two types of cryptosystems. They are the secret-key cryptosystem and the public-key cryptosystem. In secret-key encryption, the source and destination share the same key. It means the common key is used for encryption and decryption. In public-key encryption, different keys are used. In the current era of cryptographic execution, both asymmetric and symmetric cryptosystems are applied together. In this analysis, we focused on one of the standard ciphers mentioned earlier – the Hill cipher. The attack surface to cryptanalysis has extracted it unfeasible in practice; it quiet serves a vital informative role in cryptology and linear algebra [11].

In Part 2 we will describe the Literature Review. We proceeding with the aim of enhancing the Hill cipher in Part 3. Next, we discuss our proposed algorithm in Part 4. Our empirical analysis results will be presented in Part 5. Finally, we conclude in Part 6.

2 Literature Review

As it was realized, all the different methodologies (Tuti Alawiyah1, Agung Baitul Hikmah , Wildan Wiguna 2020; K. Mani,M. Viswambari, 2017; Maxrizal , Baiq Desy Aniska Prayanti, 2016; Dr. V.U.K. Sastry, K. Shirisha, 2012; Rusdhi and Mousa, 2009) were assuming that the user knew about the vulnerability and the vulnerability agents his system had to face, and do not attempt to examine their sources. Ismail, et al., [5] developed a revised Hill cipher which usages a unity matrix as a key to encode each readable blocks. In this algorithm, all readable block which know as plain text is encrypted by using its own key.

The exponentiation outcomes will be a single key which can be used for encryption. Exploration done by Rangel-Romero, et al., [6] exposed that the procedure proposed by Ismail et al. [5] consumes an insufficient

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p. 194-198
https://publishoa.com
ISSN: 1309-3452

key disadvantages which are like with the original Hill cipher. Rangel-Romero, et al., showed that the projected algorithm is quiet weak towards known plaintext attacks. Assume that the key, K used for encryption is a 2 × 2 key matrix and the initial vector, IV = [e, f]. In symmetric cryptography, attackers can easily get the encryption key since it is common practice to encrypt several plaintext blocks with a same key [4]. Assume that the attacker has successfully obtained the 2 × 2 matrix key. With this key, it is possible to calculate the IV values. Spaced out from its vulnerability to recognized readable text attack, Rangel-Romero, et al., also discussed some other drawbacks in Ismail, et al.'s algorithm. First of all, the algorithm is not suitable for all zeroes plaintext block encryption. An all zeroes plaintext block is a matrix block where all the values in it are zero. An example of a 2 × 2 all zeroes matrix. Usually, this will arise when Hill cipher is used to encode a pic which a vast portions of pixels in black. Note here that black pixels are mapped to zero in the standard grayscale image. Since the Hill cipher's linear algebra equation is C = KP (mod m), Rushdi, et al., [2]. In this algorithm, each readable block is encrypted using a random number. It will increase the randomization of the algorithm and thus increased its strength towards common attacks. This algorithm is likewise intended to evade many random numeral generation. Therefore, single one random number is generated at the beginning of encryption.

3 THE HILL CIPHER

Hill cipher is the first polygraphic cipher. A polygraphic cipher is a cipher where the plaintext is divided into groups of adjacent latters of the same fixed length n, and then each such group is transformed into a different group of n letters [11]. It has also few additional benefits in data encryption such as its resistance to frequency analysis. The fundamental of Hill cipher is matrix manipulation.

In the Hill cipher, the unreadable text is obtained from the plaintext by means of a linear transformation. The readable text which also known as plaintext row vector X is encoded as Y = KX mod m in which Y is the cipher-text row vector, K is an n×n key matrix where Kij ∈ Zm in which Zm is ring of integers modulo m where m is a natural number that is greater than one. The significance of the modulus m in the traditionally Hill cipher had 26 but its value can be optionally selected. The key matrix K is made-up to be strongly shared among the participants. The cipher-text Y is decrypted as X=Y K-1 (mod m). Such procedures are executed over Zm .

For decryption, it is to be possible that the key matrix K should be degenerated or equivalently, it should satisfy (det K (mod m), m = 1 [3]. Such range furthermore increases the key space of the cryptosystem [8].

The protectants of the Hill cipher depend on the confidentiality of the key matrix K and its rank n. If the proposed value of n was wrong, the achieved key matrix would disagree with further plaintext cipher-text pairs. The important deficiency of the Hill cipher is observed as its susceptibility to the known-plaintext attack. It can be fragmented by taking just n distinct pairs of plain-text and cipher-text [4]. In this generous attack, the cryptanalyst possesses the plaintext of some messages and the corresponding cipher text of those messages.

4 Methodology

The proposed cryptosystem includes a ciphering core that is depicted in descriptions of encryption and decryption schemes. The encryption process has the collective structure of the Affine Hill cipher but in order to give further randomization to the presented pattern and to strengthen it against the shared attacks, every chunk of data is encrypted using a random number.
Designed for avoiding several random number generations, a merely single random number is generated at the commencement of encryption and the equivalent random number of the following data chunk is repeatedly produced using a degenerated matrices key where the encryption and decryption processes should be followed from descriptions.

As of above, it is confirmed that the decode or decryption requires the inverse of the key matrix. But in some cases, the inverse of a matrix does not exist. It is a recognized statistic in the field of mathematics that the complete matrix is not invertible.

A matrix degenerated if the determinant of a matrix is zero. If the matrix has degenerated then in hill cipher, it is not conceivable to decrypt the cipher-text. In order to overwhelm the above problem, it is suggested the use of setting offset. If the determinant of a matrix is zero then set 1 as the compensated value. If the determinant is negative then set -1 as the compensated value.
A Neoteric Strategy of Hill Cipher is an efficient technique for encryption and decryption because it is easy in mathematical computation but only for a legitimate user. This is actually complex to understand and break for hackers. Neoteric Strategy of Hill Cipher further secures algorithm in a normal manner rather than other complicated hill cipher algorithm. This technique explores how vulnerability can be removing of hill cipher without using difficult mathematical computation. Because mathematical computation is very chaos to understand and implement so this is implemented in an easy manner which user can prove how it provides a solution for vulnerability in hill cipher. This A Neoteric Strategy of Hill Cipher encryption algorithm is easy in understanding and compute.

4.1 Process of Encryption

Let's P = plaintext

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p. 194-198
https://publishoa.com
ISSN: 1309-3452

K = chosen key in matrix form
compensate = is a variable
Km = modified key matrix
C = ciphertext
mod m = mod 29
mod 29 = 29 used as modulus, contain 1-26 as alphabets and 27,28 and 29 as special symbols which are more variant and beneficial from 26 used as modulus in previous work
First of all it read the simple readable text P and chosen entered key matrix K
Now in this step it find the determinant of key matrix K that is |K|
If |K| > = 0 set compensate =1 or |K| < 0 set compensate = -1
After set compensate value modified the chosen key K according to above condition
set Km instead of K after Changes in the key matrix
Find the cipher text C = Km × P mod 29
Cipher-text generated after completions of encryption process.
Then decryption processes apply on generated cipher-text.

4.2 Process of Decryption

P = plaintext,
Km = modified chosen key matrix
Km-1 is the inversion key of modified key matrix
i, j, X, Y is the variables initially set to zero
C = ciphertext
mod 29 = 29 used as modulus, contain 1-26 as alphabets and 27, 28 and 29 as special symbols which are more variant and beneficial from 26 used as modulus in previous work.
First of all it read the cipher code C and improved key matrix as Km
Find the determinant of key matrix Km set X = |Km| mod 29
If X < = 0 set X = X+ 29 or X > 0 set X = X
After set values of X find the value of i for this i × X mod 29 = = 1 this function is helpful for find the value of i
After finding value of i set it to Y = i then find the inversion of Km-1 with Km-1 = adj Km × Y mod 29
Now in the next step find the transpose of Km-1 = (Km-1)'
Finally For plain text P = C × Km-1 mod 29
If Pij < = 0 set Pij = Pij + 29 where i = 0 to 2 and j= 0

4.3 Proposed Neoteric codes for special symbols

@ = 27
. = 28
_ = 29

4.4 Flow chart of Proposed Technique

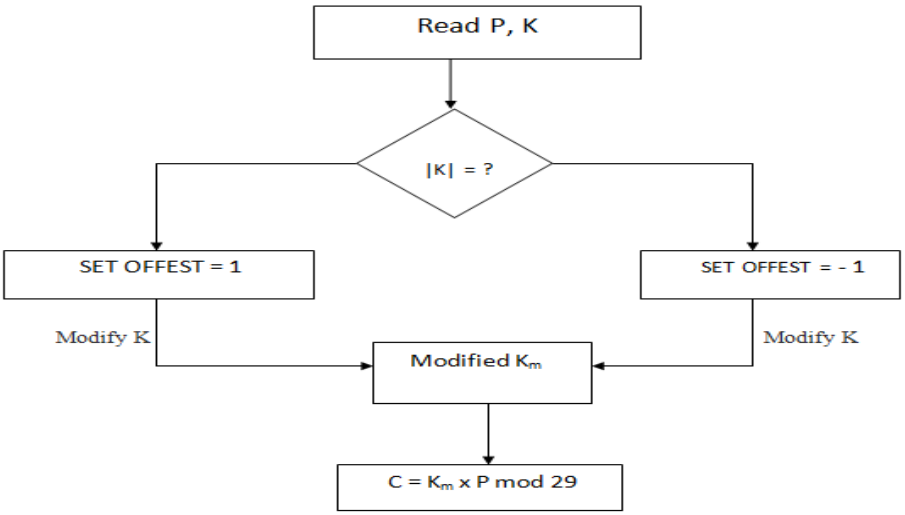

Fig: 1 Proposed Encryption Technique

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p. 194-198
https://publishoa.com
ISSN: 1309-3452

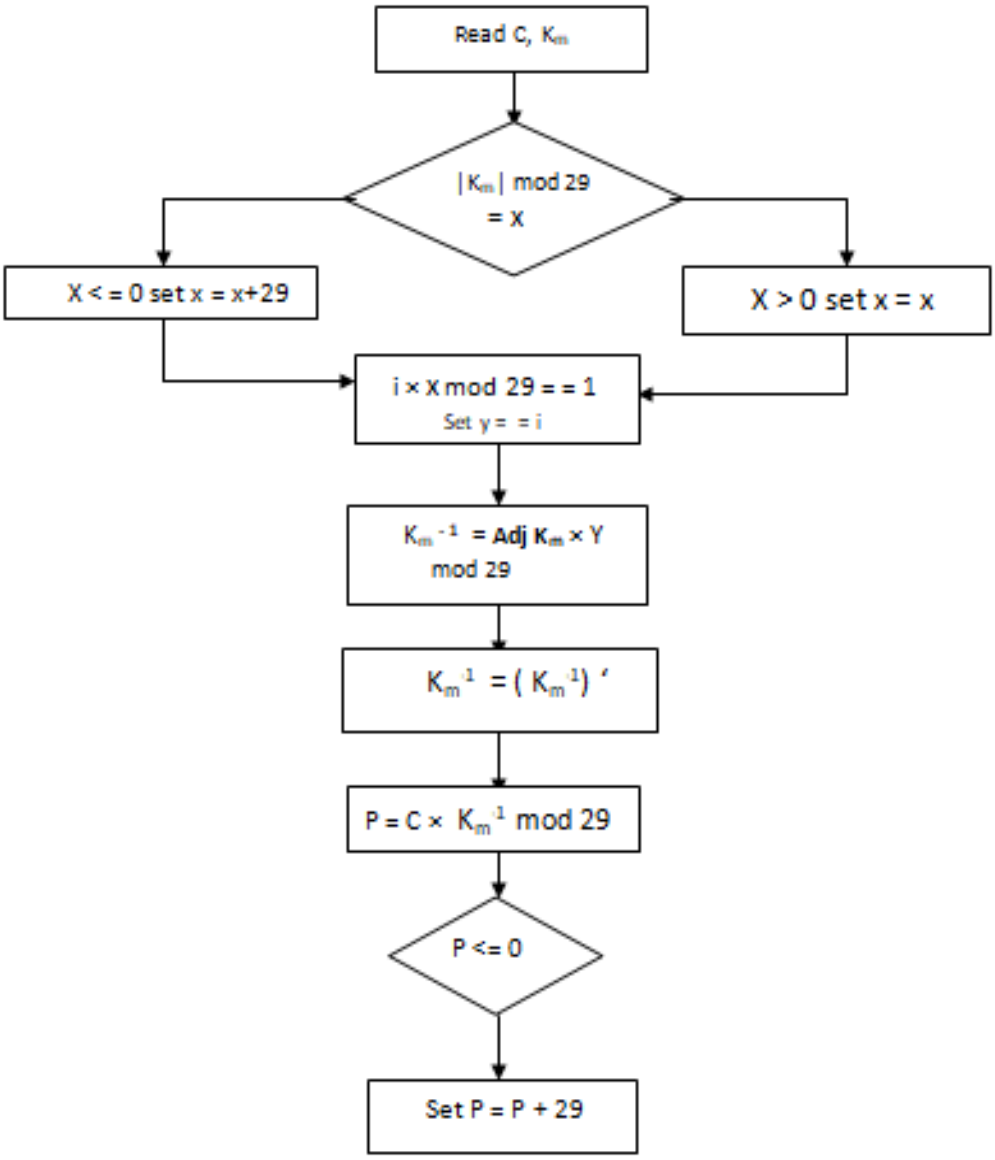

Fig: 2 Proposed Decryption Techniques

5 Result

.1 Zero vulnerability

Similarly encrypt and decrypt with the help of non-invertible key matrix of any type of plain text which have any text including special symbols between range of 27-29 of proposed alphabetical and special symbols numeric no. . Here if user take all elements zero of chosen key matrix and plain text matrix than this will also overcome zero vulnerability.

Here in output there is no margin for zero value it means here never display zero value so for zero value it will take 29 by default instead of zero value as output. We replace all elements of 29 with zero in only zero vulnerability remembers only if plain text is also 0 value then we have to assume 29 values instead of 0 values.

5.2 Using degenerated matrices

According to traditional Hill Cipher, there are several types of vulnerability raised up, here the Neoteric Strategy of hill cipher solves vulnerability of non-invertible key matrix and zero vulnerability. So Neoteric Strategy of Hill Cipher overcomes these vulnerabilities successfully. At the end of the explanation of the implementation invertible matrix provides encryption/decryption process in an easy way but using the Neoteric Strategy of Hill Cipher this simple process makes interesting because this technique uses 29 which provides a new style to plain text and ciphertext.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 1, 2022, p. 194-198
https://publishoa.com
ISSN: 1309-3452

6 Conclusions

We have presented Neoteric Strategy of Hill Cipher which is a different methodology apart version of Hill cipher. Neoteric Strategy of Hill Cipher introduces a random matrix key which is computed based on the previous cipher text blocks and a multiplying factor. This remarkably improved the obstacle of the algorithm to the recognized plaintext attack. Hill++ also implements symmetric to asymmetric key generation algorithms where the matrix key can be used for encryption and the modified key is used for decryption. By equating tentative outcomes it displays that Neoteric Strategy of Hill Cipher is the individual algorithm that justifies both evaluation factors, needs an inverse matrix key, and solves vulnerability when encrypting all zeroes plaintext block. Statistical analysis presented also shows satisfactory results. Neoteric Strategy of Hill Cipher has better encryption/decryption quality compared to the related other Hill cipher.

REFERENCES

[1] Dr. V.U.K. Sastry, K. Shirisha (2012) "A Novel Block Cipher Involving a Key Bunch Matrix" International Journal of Computer Applications, October.

[2] Rushdi, A.H. and F. Mousa(May 2009), Design of a robust cryptosystem algorithm for non-invertible matrices based on hill cipher. IJCSNS,

[3] Toorani, M. and A. Falahati (July 2009) A secure variant of the hill cipher. 40th IEEE Symposium on Computers and Communications Sousse.

[4] Stindon, D.R.,: Cryptography Theory and Practice. 3rd Edn. Chapman and Hall/CRC, 2006.

[5] Ismail, I.A., M. Amin and H. Diab (2006) How to repair the hill cipher. J. Zhejiang University. Science Academy.

[6] Rangel-Romero, Y., G. Vega-García, A. Menchaca-Méndez, D. Acoltzi-Cervantes and L. Martínez- Ramos et al.(2006) Comments on How to repair the Hill cipher. J. Zhejiang Univ. Sci. A..

[7] Bibhudendra, A.(2009) Novel methods of generating self-invertible matrix for hill cipher algorithm. International Journal of Security.

[8] Bibhudendra, A., K.P. Saroj, K.P. Sarat and P. Ganapati (2009) Image encryption using advanced hill cipher algorithm. International Journal in Recent Trends Eng..

[9] Ziedan, I.E., M.M. Fouad and D.H. Salem (2003) "Application of data encryption standard (DES) to bitmap and JPEG images, ieeexplore. Proceedings of the 20th National Radio Science Conference,.

[10] Pour, D.R., M.R.M. Said, K.A.M. Atan and M. Othman (2009) The new variable-length key Symmetric cryptosystem. Journal Mathematical Statics.

[11] Eisenberg, M (1998.) Hill ciphers and modular linear algebra. Mimeographed notes. University of Massachusetts.

[12] K. Mani, M. Viswambari (2017) "A New Method Of Hill Cipher: The Rectangular Matrix As The Private Key" Advances in Computational Sciences and Technology.

[13]Tuti Alawiyah (2020), "Genration of Rectangular Matrix Key for Hill Cipher Algorithm Using Playfair Cipher".

[14] Maxrizal, Baiq Desy Aniska Prayant (Nov 2016), "A New Method Of Hill Cipher: The Rectangular Matrix As The Private Key" International Conference on Science and Technology for Sustainability.