International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Novel Technique of Hill Cipher for Evaluation of Non-invertible key matrix

Miss Anjali saxena[1], Mr. Harsh lohiya[2], Mr. Kailash patidar[3]

[1,2,3]*computer science, shree Satay sai university*

ABSTRACT

The Hill cipher is the first polygraph cipher which has some advantages in symmetric data encryption. However, it is vulnerable to known plaintext attack. Another setback is that an invertible key matrix is needed for decryption and it is not suitable for encrypting a plaintext consisting of zeroes. The objective of this work is to modify the existing Hill cipher to overcome these issues. Studies on previous results showed that the existing Hill algorithms are not yet sufficient. Some of these algorithms are still vulnerable to known plaintext. On the other hand, some of these algorithms have better randomization properties and as a result they are more resistant against known plaintext attack. Nevertheless, these enhanced Hill cipher algorithms face the non invertible key matrix problem. Moreover, neither of these algorithms are suitable for all zeroes plaintext block encryption. In this paper, a novel technique of hill cipher is proposed which apply on invertible key matrix. A random matrix key is introduced as an extra key for encryption which has also limitations. Testing on the proposed algorithm is carried out via non-invertible key matrix approaches that are comparative different to understand. Previous research focusing on hill cipher using symmetric/asymmetric key algorithm. When user want to encrypt the message using hill cipher technique then user can do, but when user want to decrypt the message then some vulnerability arises. This study intends to use the hill cipher technique qualitative approach in evaluating the different vulnerability as inversion of key matrix. In this research user have no difficulty to find the inversion of key matrix when key matrix is invertible for decryption. In previous work there is crisis to generate the inverse key matrix when matrix is non-invertible, because when matrix is non-invertible means its determinant is zero and in hill cipher determinant plays a vital role in decryption. Then when it is zero then how user can decrypt the message. So there is requirement for such methods in which use of inversion of key matrix is possible for non-invertible matrix and which also overcome another vulnerability zero and key for modulus arithmetic.

Index Terms— Hill cipher, Encryption, Decryption, Symmetric t/Asymmetric, Vulnerability, Non-invertible, Invertible

I.INTRODUCTION

Today, information is one of the most valuable intangible assets. Due to this fact, information security has become an important issue. Cryptography is one of the methods to ensure confidentiality and integrity of information. It is from the Greek word “kryptos” which means hidden. Cryptography is the art and science of making message unintelligible. It serves as a secret communication mechanism and can be traced back till

thousands of years ago. Caesar's cipher is one of the earliest known cryptosystem which was used by Julius. All of these ciphers are the foundation for modern cryptography.

There are two types of cryptosystems. They are the symmetric cryptosystem and the asymmetric cryptosystem. In symmetric cryptosystem, the sender and recipient share the same key. It means the same key is used for encryption and decryption. In asymmetric cryptosystem, different keys are used. A public key is used by sender to encrypt the message while the recipient used a private key to decrypt it. In modern cryptographic implementation both asymmetric and symmetric cryptosystem are applied together. In this paper, we focus on one of the classical cipher mentioned earlier – the Hill cipher. Although its vulnerability to cryptanalysis has rendered it unusable in practice, it still serves as an important pedagogical role in cryptology and linear algebra [11].

Thus, a modified version of the Hill cipher will be designed to overcome the existing problems found in the cipher. In Section 2 we will discuss the background. We continue with discussing aim of enhancing the Hill cipher in Section 3. Next, we discuss our proposed algorithm in Section our empirical analysis results will be presented in Section 5. Finally, we conclude in Section 6.

II. BACKGROUND

As it was realized, all the different methodologies (Dr. V.U.K. Sastry, K. Shirisha, 2012; Rusdhi and Mousa, 2009; Toorani, M. and A. Falahati, 2009; Ismail et al, 2006; Rengel-Romero, 2006; Bibhudendra, 2006; Stindon, D.R., 2006; Ziedan, I.E., M.M. Fouad and D.H. Salem, 2003;) 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] proposed a modified Hill cipher which uses a unity (one-by-one) matrix as a key to encrypt each plaintext blocks. In this algorithm, each plaintext block is encrypted by using its own key. It is aimed to overcome the security flaw of the original Hill cipher where the same key matrix is used to encrypt all the plaintext blocks.

The multiplication results will be a unique key which can be used for encryption. Since the *IV* multiplication is performed row by row, this algorithm is known as HillMRIV (abbreviation for **H**ill **m**ultiplying **r**ows by **i**nitial **v**ector).

Research done by Rangel-Romero, *et al.*, [6] shown that the algorithm proposed by Ismail et al. [5] has a few major drawbacks which are similar with the original Hill cipher. Rangel-Romero, *et al.*, proved that the proposed algorithm is still vulnerable 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. Apart from its vulnerability to known plaintext 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 happen when Hill cipher is used to encrypt an

image which a large 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] also noticed the problem of non invertible matrix key in Hill cipher. Thus, they designed a robust cryptosystem algorithm for non invertible matrices. Toorani, *et al.,* [3] created a variant of Hill cipher which is an extension of the Bibhudendra (self invertible key matrix) [7]. In this algorithm, each plaintext 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 also aimed to avoid multiple random number generation. Thus, only one random number is generated at the beginning of encryption.

III.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]. This polygraphic feature increased the speed and throughput of Hill cipher. Besides, it has some other advantages in data encryption such as its resistance to frequency analysis. The core of Hill cipher is matrix manipulation.

In the Hill cipher, the ciphertext is obtained from the plaintext by means of a linear transformation. The plaintext row vector **X** is encrypted as **Y = KX** mod *m* in which **Y** is the ciphertext row vector, **K** is an *n*×n key matrix where **K*ij* ∈ Zm** in which **Zm** is ring of integers modulo *m* where *m* is a natural number that is greater than one. The value of the modulus *m* in the original Hill cipher was 26 but its value can be optionally selected. The key matrix **K** is supposed to be securely shared between the participants. The ciphertext **Y** is decrypted as **X=Y K-1 (**mod *m).* All operations are performed over **Zm .**

For decryption to be possible, the key matrix **K** should be invertible or equivalently, it should satisfy (det **K** (mod *m), m* = 1 [3]. However, many of square matrices are not invertible over. The risk of determinant having common factors with the modulus can be reduced by taking a prime number as the modulus. Such selection also increases the key space of the cryptosystem [8].

The security of the Hill cipher depends on confidentiality of the key matrix **K** and its rank *n*. If the guessed value of *n* was incorrect, the obtained key matrix would be disagreed with further plaintext- ciphertext pairs. The most important security flaw of the Hill cipher is regarded to its vulnerability to the known-plaintext attack. It can be broken by taking just *n* distinct pairs of plaintext and ciphertext [4]. In this kind of attack, the cryptanalyst possesses the plaintext of some messages and the corresponding ciphertext of those messages. He will try to deduce the key or an algorithm to decrypt any new messages encrypted with the same key.

IV.THE PROPOSED SCHEME FOR EVALUATION OF NON INVERTIBLE KEY MATRIX

The proposed cryptosystem includes a ciphering core that is depicted in descriptions of encryption and decryption scheme. The encryption core has the same structure of the Affine Hill cipher but in order to give more randomization to the introduced scheme and to strengthen it against the common attacks, each block of data is encrypted using a random number. For avoiding multiple random number generations, only one random

number is generated at the beginning of encryption and the corresponding random number of the following data blocks is recursively generated using a non invertible key matrix where the encryption and decryption procedures should be followed from descriptions.

From above it is clear that the decryption requires the inverse of the key matrix. But in some cases the inverse of a matrix does not exist. It is a well known fact in the field of mathematics that the entire matrix is not invertible.

A matrix is non invertible if the determinant of a matrix is zero. Also if matrix is non invertible then in hill cipher, it is not possible to decrypt the cipher text. In order to overcome the above problem, it is suggested the use of setting offset**.** If the determinant of a matrix is zero then set 1 as the compensate value. If the determinant is negative then set -1 as the compensate value.

Novel technique of hill cipher is time consuming technique for encryption and decryption because it is easy in mathematical computation but only for authorized person. This is very complicated to understand and breaking for hackers. Novel hill cipher more secure algorithm in easy manner rather than other complicated hill cipher algorithm. This technique prove that how vulnerability can be overcome of hill cipher without using the complicated mathematical computation. Because mathematical computation is very chaos to understand and implement so this is implemented in easy manner which user can prove how it is provide solution for vulnerability in hill cipher. This novel technique of hill cipher encryption algorithm is easy in understand and computed.

4.1 Process of Encryption

Let's **P = plaintext**

K = chosen key in matrix form

compensate = is a variable

Km = modified key matrix

C = **ciphertext**

mod m = mod 33

mod 33 = 33 used as modulus, contain 1-26 as alphabets and 27-33 as special symbols which are more variant and beneficial from 26 used as modulus in previous work

i) Firstly read the plain text P and chosen key matrix K
ii) Find the determinant of key matrix K that is |K|

iii) If |K| > = 0 set compensate =1 or |K| < 0 set compensate = -1

iv) After set compensate value modified the chosen key K according to above condition

v) set K to Km after modify the key matrix

vi) Find the cipher text C = Km × P mod 33

Ciphertext generated after completions of encryption process.

Then decryption processes apply on generated ciphertext.

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 33 = 33 used as modulus, contain 1-26 as alphabets and 27-33 as special symbols which are more variant and beneficial from 26 used as modulus in previous work.

i) Firstly read the Cipher text C and modified key matrix as K**m**

ii) Find the determinant of key matrix K**m** set X = |K**m**| mod 33

iii) If X < = 0 set X = X+ 33 or X > 0 set X = X

iv) After set values of X find the value of i for this i × X mod 33 = = 1 this function is helpful for find the value of i

v) After finding value of i ser it to Y = i then find the inversion of Km-1 with Km-1 = adj Km × Y mod 33

vi) Now next step shows transpose of Km-1 = (K**m-1**)**'**

vii) Finally For plain text P = C × Km-1 mod 33

viii) If P**ij** < = 0 set P**ij = Pij** + 33 where i = 0 to 2 and j= 0

4.3 Proposed novel codes for special symbols

, = 2 7	. = 2 8	_ = 2 9	- = 3 0	? = 3 1	\ = 3 2	: = 3 3

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

V.ANALYSIS

5.1 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 1-33 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 33 by default instead of zero value as output. We replace all elements of 33 with zero in only zero vulnerability remembers only if plain text is also 0 value then we have to assume 33 values instead of 0 values.

5.2 Using invertible matrix

According to hill cipher there are various types of vulnerability raised, here novel version of hill cipher solve Vulnerability of non invertible key matrix and zero vulnerability. So novel version of hill cipher overcome these vulnerability successfully. At the end of explanation of implementation invertible matrix provide encryption/decryption process in easy way but using novel version of hill cipher this simple process make interesting because this technique using 33 which provide new style to plain text and cipher text.

5.3 Comparison chart with existing algorithm.

This comparison chart provides that how various types of hill cipher algorithm achieved which vulnerabilities

TABLE 1

Comparison chart with various factors

Cipher algorithm	Comparison factor		
	Need inverse key matrix	Solution for non invertible key matrix	Vulnerable if there all zeros block
Original Hill cipher	Yes	No	Yes
Ismail, et al's algo	Yes	Yes	Yes
Rushdi, et al's algo	Yes	Yes	Yes
Bibhudendra , et al's algo	Yes	Yes	Yes
Novel hill cipher	Yes	Yes	No

VI.CONCLUSIONS

We have presented a novel version of Hill cipher which is an different methodology apart versions of Hill cipher. Novel hill cipher introduces a random matrix key which is computed based on the previous ciphertext blocks and a multiplying factor. This significantly increased the resistance of the algorithm to the known plaintext attack. Hill++ also implements a symmetric to asymmetric key generation algorithm where the matrix key can be used for encryption and modified key is used for decryption. By comparing experimental results it shows that Novel Hill cipher is the only algorithm which fulfills both comparison factors, need an inverse matrix key and it is solve vulnerability when encrypting all zeroes plaintext block. Statistical analysis presented also shows satisfactory results. Novel Hill cipher has better encryption/decryption quality compared to the related other Hill cipher

Acknowledgment

REFERENCES

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

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

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

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

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

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

[7] Bibhudendra, A.: Novel methods of generating selfinvertible matrix for hill cipher algorithm. International Journal of Security, 2009.

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

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

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

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