A Novel Approach to Hill Cipher

Neha Sharma
Department of Computer Science and Engineering
Oriental University, Indore
India

Sachin Chirgaiya
Department of Computer Science and Engineering
Oriental University, Indore
India

ABSTRACT
Hill Cipher is a first polygraphic substitution cipher that works on digraphs, trigraphs (3 letter squares) or hypothetically blocks of any magnitude. The Hill Cipher utilizes a region of science called Linear Algebra, and specifically requires the client to have a rudimentary knowledge of matrices. It additionally makes utilization of Modulo Arithmetic (like the Affine Cipher). To perform decryption, the hill cipher requires the inverse of the key matrix. This is the major shortcoming of Hill cipher since every key matrix is not invertible. We will propose a new variant of hill cipher, which will find the decryption of the cipher text even when the key matrix is non invertible.

General Terms
Cryprography, encryption, decryption, Hill Cipher, modulo 26, digraphs, trigraphs

Keywords
Hill Cipher, Invertible key matrix, offset, determinant.

1. INTRODUCTION
In this era of worldwide electronic connectivity, of hackers as well as viruses, of electronic snooping and electronic hoax, there is certainly a need to save the data safely. This will lead to a keen attentiveness to protect resources and information from exposure, to assure the authenticity of messages and information, and to safeguard systems from network-based attacks [1]. Cryptography, the art of encryption, plays a major part in cellular communications, e-commerce, computer passwords, pay-tv, sending emails; ATM cards security, transmitting funds, digital signatures and touches numerous sides of our day to day lives. Cryptography is the science or art of encircling the techniques and principles of converting an understandable message (plaintext) into one that is making no sense (cipher text) and then reconverting that message again to its original form. Nowadays, cryptography is considered as a branch of computer science as well as mathematics, and is associated strongly with computer security, engineering and information theory. Even though, long-ago cryptography referred only to the decryption and encryption of message using secret keys. At the present time, cryptography is usually classified into two major categories, symmetric and asymmetric. In symmetric cryptography, the sender and receiver both use the same key for encryption and decryption while in asymmetric cryptography, two different keys are used. Both of these cryptosystem have their own advantages and disadvantages. For illustration, Symmetric cryptography uses a smaller amount computing power but it is less intact than Asymmetric cryptography. Currently, there are only some cryptosystem which are widely employed such as Advanced Encryption Standard (AES), Twofish, River Cipher 4 (RC4) and Data Encryption Standard (DES). On the other hand, these contemporary cryptosystem have their genesis. The conventional cipher such as Caesar Cipher, Hill Cipher, Vigenere Cipher provides the base for the cryptology's world in our day. In this paper, we focus on Hill Cipher which was first developed by the mathematician Lester S. Hill, in 1929 and was published in the journal The American Mathematical Monthly (Eisenberg, 1998). Even though its vulnerability to cryptanalysis has rendered it unusable in practice, it still serves an important pedagogical role in cryptology and linear algebra [2]. Therefore, a modified version of Hill cipher will be proposed to overcome the drawbacks of the existing algorithm.

2. HILL CIPHER
The Hill Cipher was imagined by Lester S. Hill in 1929, and like the other Digraphic Ciphers it follows up on gatherings of letters. Not at all like the others, however, it is extendable to take a shot at distinctive estimated pieces of letters. In this way, actually it is a polygraphic substitution cipher, that works on digraphs, trigraphs (3 letter squares) or hypothetically blocks of any magnitude.

The Hill Cipher utilizes a region of science called Linear Algebra, and specifically requires the client to have a rudimentary knowledge of matrices. It additionally makes utilization of Modulo Arithmetic (like the Affine Cipher). As a result of this, the cipher has an extensively more numerical nature than a portion of the others. This characteristic of Hill permits it to act (moderately) effortlessly on bigger pieces of letters.

2.1 Working of Hill Cipher
Hill Cipher works by assigning a numerical value to each letter of the word. In English language, we have 26 alphabets, therefore Hill also works on modulo 26 and we will utilize the standard 26 alphabets in order and derive the following relationship between letters and numbers.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

2.1.1 Encryption
For encrypting a message utilizing the Hill Cipher, we should first transform our word into a key matrix (a 2 x 2 lattice for working with digraphs, a 3 x 3 lattice for working with trigraphs, and so forth). We additionally transform the plaintext into digraphs (or trigraphs) and all of these into a column vector. We then carry out matrix multiplication, modulo the length of the letters in order (i.e. 26) on every vector. These vectors are then translated into letters to deliver the ciphertext.

To understand the encryption procedure let us take an example, we will encrypt the plaintext "party here" using the key matrix "back up abc" with a 3x3 matrix.

2.1.1.1 Now we will turn our Key Matrix in its Corresponding Numerical Value.

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}$$

2.1.1.2 Now We Break the Plaintext into Trigraphs

Because we are using 3x3 matrixes, therefore we will group our message into 3 letters, and convert them into a column vectors. If the string is not completely divisible by 3 then add a predetermined character at the end of the string.

$$\begin{pmatrix} P \\ A \\ R \end{pmatrix} = \begin{pmatrix} 15 \\ 0 \\ 17 \end{pmatrix}$$

$$\begin{pmatrix} T \\ Y \\ H \end{pmatrix} = \begin{pmatrix} 19 \\ 24 \\ 7 \end{pmatrix}$$

$$\begin{pmatrix} E \\ R \\ E \end{pmatrix} = \begin{pmatrix} 4 \\ 17 \\ 4 \end{pmatrix}$$

2.1.1.3 Now we will multiply each of these Column Vectors by our Key Matrix and after that we will take modulo 26 of the Result.

$$\begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 15 \\ 0 \\ 17 \end{pmatrix} = \begin{pmatrix} 49 \\ 405 \\ 34 \end{pmatrix} = \begin{pmatrix} 23 \\ 15 \\ 8 \end{pmatrix} \text{ (modulo 26)}$$

$$\begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 19 \\ 24 \\ 7 \end{pmatrix} = \begin{pmatrix} 33 \\ 775 \\ 38 \end{pmatrix} = \begin{pmatrix} 7 \\ 21 \\ 12 \end{pmatrix} \text{ (modulo 26)}$$

$$\begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 4 \\ 17 \\ 4 \end{pmatrix} = \begin{pmatrix} 12 \\ 440 \\ 25 \end{pmatrix} = \begin{pmatrix} 12 \\ 24 \\ 25 \end{pmatrix} \text{ (modulo 26)}$$

2.1.1.4 Now we will again convert the column matrices into their corresponding alphabets and combine them to obtain the ciphertext.

$$\begin{pmatrix} 23 \\ 15 \\ 8 \end{pmatrix} = \begin{pmatrix} X \\ P \\ I \end{pmatrix}$$

$$\begin{pmatrix} 7 \\ 21 \\ 12 \end{pmatrix} = \begin{pmatrix} H \\ V \\ M \end{pmatrix}$$

$$\begin{pmatrix} 12 \\ 24 \\ 25 \end{pmatrix} = \begin{pmatrix} M \\ Y \\ Z \end{pmatrix}$$

Ciphertext--- XPIHVMMYZ

From the encryption process of Hill Cipher, we encrypted the text "PARTYHERE" to "XPIHVMMYZ"

2.1.2 Decryption

For decrypting a ciphertext encoded utilizing the Hill Cipher, we need to calculate the inverse of the key matrix. After that the process is same as the done for the encryption. Once we got the inverse of the key matrix, we multiply it by the column vectors in which the ciphertext is part into, take the results modulo the length of the letters in order, and lastly change over the numbers again to letters.

Since most of the methodology is the same as encryption, we are going to concentrate on discovering the inverse of the key matrix, and will then skim rapidly through further steps.

All in all, to discover the inverse of the key matrix, we perform the following computation,

$K^{-1}=d^{-1}$ x adj(K)

Where,

K= key matrix,

d= determinant of the key matrix

adj(k)= adjugate matrixof K.

To understand the decryption procedure let us proceed with our previous example, we will decrypt the ciphertext "XPIHVMMYZ" using the key matrix "back up abc" with a 3x3 matrix. Following are the steps invove in decryption.

2.1.2.1 Find the Multiplicative Inverse of the Determinant

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}$$

Now calculate the determinant of the key matrix.

$$\begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix} = +1\begin{pmatrix} 20 & 15 \\ 1 & 2 \end{pmatrix} - 0\begin{pmatrix} 10 & 15 \\ 0 & 2 \end{pmatrix} + 2\begin{pmatrix} 10 & 20 \\ 0 & 1 \end{pmatrix}$$

$$= +1(40\text{-}15) - 0\,(20\text{-}0) + 2\,(10\text{-}0)$$

$$= 25 - 0 + 20$$

$$= 45$$

$$= 19(\text{modulo } 26)$$

We now have to find the multiplicative inverse of the determinant working modulo 26. That is, the number between 1 and 25 that gives an answer of 1 when we multiply it by the determinant. So, in this case, we are looking for the number that we need to multiply 19 by to get an answer of 1 modulo 26. There are algorithms to calculate this, but it is often easiest to use trial and error to find the inverse.

$dd^{-1}=1(\text{modulo}26)$

$19* X=1(\text{modulo } 26)$

$19x11=209= 1(\text{modulo } 26)$

So, 11 is the multiplicative inverse of the determinant of the key matrix.

2.1.2.2 Find the Adjugate Matrix

$$\text{Adj}\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} +\begin{pmatrix} e & f \\ h & i \end{pmatrix} & -\begin{pmatrix} b & c \\ h & i \end{pmatrix} & +\begin{pmatrix} b & c \\ e & f \end{pmatrix} \\ -\begin{pmatrix} d & f \\ g & i \end{pmatrix} & +\begin{pmatrix} a & c \\ g & i \end{pmatrix} & -\begin{pmatrix} a & c \\ d & f \end{pmatrix} \\ +\begin{pmatrix} d & e \\ g & h \end{pmatrix} & -\begin{pmatrix} a & b \\ g & h \end{pmatrix} & +\begin{pmatrix} a & b \\ d & e \end{pmatrix} \end{pmatrix}$$

Adj

$$\begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} +\begin{pmatrix} 20 & 15 \\ 1 & 2 \end{pmatrix} & -\begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix} & +\begin{pmatrix} 0 & 2 \\ 20 & 15 \end{pmatrix} \\ -\begin{pmatrix} 10 & 15 \\ 0 & 2 \end{pmatrix} & +\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} & -\begin{pmatrix} 1 & 2 \\ 10 & 15 \end{pmatrix} \\ +\begin{pmatrix} 10 & 20 \\ 0 & 1 \end{pmatrix} & -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & +\begin{pmatrix} 1 & 0 \\ 10 & 20 \end{pmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} +25 & +2 & -40 \\ -20 & +2 & +5 \\ +10 & -1 & +20 \end{pmatrix}$$

$$= \begin{pmatrix} +25 & +2 & +12 \\ +6 & +2 & +5 \\ +10 & +25 & +20 \end{pmatrix} \text{(modulo 26)}$$

2.1.2.3 Multiply the Multiplicative Inverse of the Determinant by the Adjugate Matrix

$$11 \times \begin{pmatrix} 25 & 2 & 12 \\ 6 & 2 & 5 \\ 10 & 25 & 20 \end{pmatrix} = \begin{pmatrix} 275 & 22 & 132 \\ 66 & 22 & 55 \\ 110 & 275 & 220 \end{pmatrix}$$

$$= \begin{pmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{pmatrix} \text{(modulo 26)}$$

That is,

$$\text{If } K = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}, \text{ then } K^{-1} = \begin{pmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{pmatrix}$$

2.1.2.4 We have the Inverse of the Key, now we will multiply our Cipher text Column Vectors with it.

$$\begin{pmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{pmatrix} \begin{pmatrix} 23 \\ 15 \\ 8 \end{pmatrix} = \begin{pmatrix} 691 \\ 676 \\ 459 \end{pmatrix} = \begin{pmatrix} 15 \\ 0 \\ 17 \end{pmatrix} \text{(modulo 26)}$$

$$\begin{pmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{pmatrix} \begin{pmatrix} 7 \\ 21 \\ 12 \end{pmatrix} = \begin{pmatrix} 591 \\ 596 \\ 501 \end{pmatrix} = \begin{pmatrix} 19 \\ 24 \\ 7 \end{pmatrix} \text{(modulo 26)}$$

$$\begin{pmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{pmatrix} \begin{pmatrix} 12 \\ 24 \\ 25 \end{pmatrix} = \begin{pmatrix} 758 \\ 771 \\ 732 \end{pmatrix} = \begin{pmatrix} 4 \\ 17 \\ 4 \end{pmatrix} \text{(modulo 26)}$$

2.1.2.5 Now we will again convert the column matrices into their corresponding alphabets and combine them to obtain the plaintext.

$$\begin{pmatrix} 15 \\ 0 \\ 17 \end{pmatrix} = \begin{pmatrix} P \\ A \\ R \end{pmatrix}$$

$$\begin{pmatrix} 19 \\ 24 \\ 7 \end{pmatrix} = \begin{pmatrix} T \\ Y \\ H \end{pmatrix}$$

$$\begin{pmatrix} 4 \\ 17 \\ 4 \end{pmatrix} = \begin{pmatrix} E \\ R \\ E \end{pmatrix}$$

Plaintext-"PARTYHERE"

And we get our Original Plaintext-"PARTYHERE". Here, we have decrypted our ciphertext back into original plaintext but space has been removed, we can either manually add space between alphabets or we can dedicate certain character for space, for eg "¬" has been assigned to space, then we have to follow modulo 27 in place of modulo 26.

2.2 Analysis of Hill Cipher

The most essential thing that must be talked about with respect to the utilization of the Hill Cipher is that not every conceivable matrix is a conceivable key matrix. This is on the grounds that, to decrypt, we need an inverse key matrix, and not every matrix is invertible. Luckily, we don't need to work out the whole inverse to discover it is unrealistic, however basically consider the determinant. 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 such case, some other key is chosen; this is the major drawback of the Hill Cipher.

To understand this problem, let us take an example of an non-invertible key matrix.

Suppose,

$$\text{If } K = \begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix}$$

Then

$$\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix} = +2\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} - 2\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} + 2\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$$

$$= 2\,(4-4) - 2\,(4-4) + 2\,(4-4)$$

$$= 0$$

The Hill Cipher will not be able to decrypt it because the determinant of our Key matrix will be zero.

3. PROPOSED ALGORITHM

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, we suggest the use of setting offset. If the determinant of a matrix is zero then set 1 as the offset value. If the determinant is negative then set -1 as the offset value.

3.1 Encryption Algorithm

The steps of the encryption algorithm are as follows:

Step1: Start

Step 2: Input: Plaintext, Key Matrix,

Step 3: Convert the plaintext characters in to matrix form P

Step 3: Perform Encryption using

C = KP MOD 26

Where C & P are the matrices of order 1 X N. Also K is a matrix of the order NXN.

3.2 Decryption Algorithm

The steps of the Decryption algorithm are as follows:

Step1: Start

Step 2: Input : Ciphertext, Key matrix

Step 3: Calculate inverse key. If the determinant of the Key matrix is zero> Then set offset as follows:

If (Determinant > =0)

Then set offset =1

Else

Set offset = -1

Step 4: Decryption: $P = CK^{-1}$ Mod 26

4. EXAMPLE TEST CASE

S NO.	KEY VALUES	MESSAGE	CIPHERTEXT	PLAINTEXT
1	{{2,2,2},{2,2,2},{2,2,2}}	{13,1,8}	{5,19,26}	{13,1,8}
2	{{1,2,1},{1,2,1},{1,2,1}}	{13,1,8}	{10,24,5}	{13,1,8}
3	{{12,12,12},{12,12,12},{12,12,12}}	{13,1,8}	{17,5,12}	{13,1,8}
4	{{11,11,11},{12,12,12},{11,11,11}}	{13,1,8}	{21,5,16}	{13,1,8}
5	{{2,2,2},{6,6,6},{6,6,6}}	{13,1,8}	{5,3,10}	{13,1,8}

In our example we have taken 5 different key matrices, each of which having the determinant zero, Hill Cipher is not able to decrypt such key matrices but by taking offset we can encrypt and decrypt our message.

5. CONCLUSION

In this paper we have discussed about the limitations of the present version of Hill cipher. Then we proposed a unique offset based solution for the decryption and we conclude that [-1, 1] on the basis of all randomized values of key. We found that the results are similar in the case of different key values. So, we conclude that [-1, 1] are enough key values for getting a solution and our proposed solution has the ability to decrypt the plaintext effectively even if k equals zero.

6. ACKNOWLEDGMENTS

Special thanks to Oriental University, my guide Prof. Sachin Chirgaiya and Department of Computer Science and Engineering, Oriental University for their support and guidance.

7. REFERENCES

[1] William Stallings " Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2] Al-Saidi, N.M.G. and M.R.M. Said, 2009. A new approach in cryptographic systems using fractal image coding. J. Math. Stat., 5: 183-189. DOI: 10.3844/jmssp.2009.183.189

[3] Bibhudendra, A., 2006. Novel methods of generating self-invertible matrix for hill cipher algorithm. Int. J. Secur., 1: 14-21. http://dspace.nitrkl.ac.in:8080/dspace/handle/2080/ 620

[4] Bibhudendra, A., K.P. Saroj, K.P. Sarat and P. Ganapati, 2009. Image encryption using advanced hill cipher algorithm. Int. J. Recent Trends Eng., 1: 663-667. http://www.ijrte.academypublisher.com/vol01/no0 1/ijrte0101663667.pdf

[5] Eisenberg, M., 1998. Hill ciphers and modular linear algebra. Mimeographed notes. University of Massachusetts. http://www.apprendre-enligne. net/crypto/hill/Hillciph.pdf

[6] Ismail, I.A., M. Amin and H. Diab, 2006. How to repair the hill cipher. J. Zhejiang Univ. Sci. A., 7: 2022- 2030. DOI: 10.1631/jzus.2006.A2022

[7] Pour, D.R., M.R.M. Said, K.A.M. Atan and M. Othman, 2009. The new variable-length keysymmetric cryptosystem. J. Math. Stat., 5: 24-31. DOI: 10.3844/jmssp.2009.24.31

[8] 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., 9: 211- 214. DOI: 10.1631/jzus.A072143

[9] Rushdi, A.H. and F. Mousa, 2009. Design of a robust cryptosystem algorithm for non-invertible matrices based on hill cipher. Int. J. Comput. Sci. Network Secur., 9: 11-16 http://paper.ijcsns.org/07_book/200905/20090502. pdf