IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-2 E-ISSN: 2347-2693

# Enhancing Resistance of Hill Cipher using Columnar and Myszkowski Transposition

Anirban Bhowmick[1] and Geetha M[2]
[1]Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal, India
[2] Professor, Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal, India

www.ijcaonline.org

Received: Feb /17/2015 Revised: Feb/20/2015 Accepted: Feb/23/2015 Published: Feb/28/ 2015

***Abstract*—** Researchers are regularly trying to figure out secure encryption algorithms so that the data transmitted over the computer networks are not intercepted by an unwanted entity.. The two methods to encrypt data are- Transposition and Substitution. Transposition refers to changing the position of characters in a given text. On the other hand, substitution is the process of replacing each character of the plaintext with some other character. One main concern area is to the existing encryption system to overcome the flaws in them.

In this paper, an emphasis is given on enhancement of security of hill cipher algorithm. This algorithm uses simple substitution method and resistance is improved by applying columnar and Myszkowski transpositions.

***Keywords*—** Cryptography, Encryption, Modified Hill Cipher, Columnar Transposition, Myszkowski Transposition.

## I. INTRODUCTION

Communication between the sender and the receiver needs security. Whenever there are two entities communicating, the large sized data being conveyed should be encrypted. Cryptography was introduced to provide the data confidentiality [1]. Cryptography is of two types - Secret Key Cryptography and Public Key Cryptography [2] [13].

Encryption, one of the aspects of cryptography, scrambles the data beyond recognition. This provides data security [3] from intruders. Once the data is encrypted, it can be transmitted over the network. It can be then decrypted, at the receiver's end, to obtain the original data. The algorithm used for encrypting the data should be simple, strong and secure.

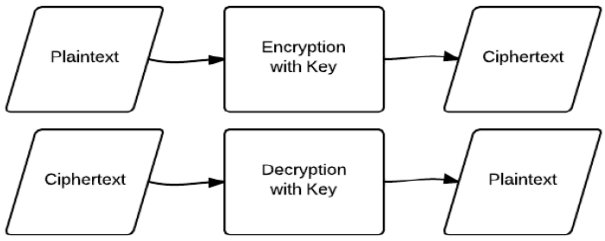


Fig 1: Encryption and Decryption process

Hill cipher is a polygraphic substitution [4] cipher based on linear algebra. Each alphabet is of the plain text will be substituted by another alphabet and this replacement is determined by a cipher key. Each alphabet is represented by a number modulo 26 as shown in the Table1.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| A | B | C | D | E | F | G | H | I | J |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| K | L | M | N | O | P | Q | R | S | T |
| 20 | 21 | 22 | 23 | 24 | 25 | | | | |
| U | V | W | X | Y | Z | | | | |

Table 1: Alphabet matrix

To encrypt a message, each block of $n$ letters is multiplied by an invertible $n \times n$ matrix, again modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption. The matrix used for encryption is the cipher key, and it should be selected randomly from the set of invertible $n \times n$ matrices.

Consider for example the
Cipher Key

$$\begin{pmatrix} 9 & 19 \\ 1 & 6 \end{pmatrix}$$

And a Plain text: COST

$$\begin{pmatrix} C \\ O \end{pmatrix} \begin{pmatrix} S \\ T \end{pmatrix} \rightarrow \begin{pmatrix} 2 \\ 14 \end{pmatrix} \begin{pmatrix} 18 \\ 19 \end{pmatrix}$$

© 2015, IJCSE All Rights Reserved 

The Encryption of CO is YI and is described below

$$\begin{pmatrix} 9 & 19 \\ 1 & 6 \end{pmatrix} \begin{pmatrix} 2 \\ 14 \end{pmatrix} \rightarrow \begin{pmatrix} 284 \\ 86 \end{pmatrix} \text{(mod 26)} \rightarrow \begin{pmatrix} 24 \\ 8 \end{pmatrix} \rightarrow \begin{pmatrix} Y \\ I \end{pmatrix}$$

Similarly, Decryption of YI uses the inverse of the cipher key used for encryption. Therefore,

$$\begin{pmatrix} 9 & 19 \\ 1 & 6 \end{pmatrix}^{-1} \rightarrow \begin{pmatrix} 18 & 21 \\ 23 & 27 \end{pmatrix} \text{(mod 26)}$$

$$\begin{pmatrix} 18 & 21 \\ 23 & 27 \end{pmatrix} \begin{pmatrix} 24 \\ 8 \end{pmatrix} \rightarrow \begin{pmatrix} 600 \\ 768 \end{pmatrix} \rightarrow \begin{pmatrix} 2 \\ 14 \end{pmatrix} \text{(mod 26)} \rightarrow \begin{pmatrix} C \\ O \end{pmatrix}$$

The basic hill cipher is vulnerable to known-plaintext attack [5] because it is completely linear. To improve the resistance of hill cipher from such attacks, columnar transposition and Myszkowski transposition are applied on hill cipher.

Columnar transpositions [6] are of two types – Regular and irregular. In this paper, regular columnar transposition is used and in which spaces are ignored from the plain text. Columnar transposition is a technique in which the plain text is written in a matrix in row-wise manner. The cipher text is obtained by reading this matrix column-wise. The order in which the columns are read is decided by a key.

Myszkowski transposition [7] is a variation to columnar transposition. Again, in this case, the plain text is written in a matrix in row-wise manner and read column-wise. The order of reading the columns is decided by the key but this key can have repeating numbers unlike the key for columnar transposition. Plaintext columns with unique numbers are transcribed downward but those with recurring numbers are transcribed left to right.

Section 2 gives the literature survey in the field of enhancing hill cipher. Section 3 describes the proposed algorithm. The working of the proposed algorithm is discussed in section 4. Section 5 compares the proposed algorithm with the classical hill cipher algorithm and Section 6 concludes the paper.

## II. RELATED WORK

Over the years, significant attempts have been to improve the resistance of hill cipher and numerous applications of hill cipher have also been suggested.

Authors in [8] have proposed the use of dynamic key matrix, achieved by random permutations of columns and rows of the master key matrix, as the cipher key matrix. The number of dynamic keys generated is m! where m refers to the size of the key matrix. In this case, the encrypted text and the permutation vector are sent to the receiver.

Authors in [9] work the same way as the algorithm in [8] but transfer of the permutation vector is not done here, instead both the sender and the receiver use a pseudo-random permutation generator. In this case only the number of the necessary permutation is transferred to the receiver. The number of dynamic keys is the same as that of [8].

Authors in [10] have strengthened the security of hill cipher by making the use of elements of finite fields and logical XNOR operator.

Authors in [11] have also made an attempt to enhance the security of hill cipher. The method employed generates variable-length key matrices from a given shared Maximum Distance Separable (MDS) master key matrix. With the matrices generated, each plaintext matrix is encrypted using a separate key matrix which improves resistance of the cipher text against known plaintext attack.

Authors in [12] have suggested an improvement in hill cipher. Hill cipher always needs a key matrix which is invertible. To overcome this problem, this paper provides a setting offset. The offset value is 1 when determinant is 0 and -1 when determinant is negative.

## III. PROPOSED TECHNIQUE

### *A. Encryption*

The proposed symmetric encryption algorithm will necessitate three keys to convert plain text to cipher text. The first key ($K_1$) will be a matrix key. Each alphabet of the plain text is represented by a numeric value. These numeric values are placed in a matrix. Multiplication of the key matrix with the plain text matrix will produce an intermediary cipher text matrix which is subjected to modulo operation to obtain the final cipher matrix allowing substitution of each alphabet in the plaintext. After the replacement of each alphabet in the plaintext is done, the


© 2015, IJCSE All Rights Reserved

first intermediary cipher text ($C_1$) is obtained. In case of classical hill cipher, this cipher text ($C_1$) would have been the final encrypted text.

In this proposed algorithm as shown in figure1, columnar transposition is applied to $C_1$ using key $K_2$. The second key ($K_2$) will be a string of non-repeating numbers. The number of digits constituting the length of key $K_2$ is calculated. $C_1$ is then written out in rows of the same length as the number of digits in $K_2$. The second intermediary text ($C_2$) is obtained by reading the text in column by column manner. The order in which the columns are read is decided by the key $K_2$.

The third key ($K_3$) will be a string of repeating or non-repeating numbers. Again, the number of digits constituting the length of key $K_3$ is calculated. The second intermediary text ($C_2$) is written out in row by row manner with each row having the same length as the length of key $K_3$. The matrix is then read column by column to obtain the final cipher text (C). The columns are transcribed downwards which have unique numbers but those which are repeating are read from left to right.

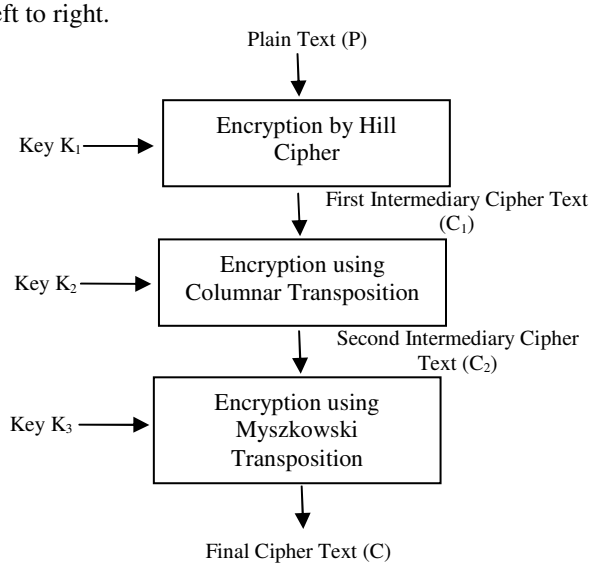


Fig 2: Proposed Encryption Steps

B. *Decryption*

Symmetric cryptographic algorithms share the same set of keys during encryption and decryption. In such cases, decryption is just the reverse process. During decryption, all the three keys are used again but this time in the reverse order.

The first key to be used will be $K_3$. The cipher text is written in column by column manner. The order in which the text is written out into columns is decided by the key ($K_3$). The key being used in this case may have repeating numbers. For unique column numbers, the characters are written downwards but for the repeating column numbers, the characters are written from left to right. Then the matrix formed is read in row-wise manner to obtain the first intermediary plain text ($P_1$).

This plain text ($P_1$) is written out in another matrix using key $K_2$. The characters are written column by column in this case. The column order is again decided by the key $K_2$. The characters are then read in row by row manner to obtain the next plain text ($P_2$).

This plain text ($P_2$) is the text decrypted using hill cipher. The inverse of the key matrix is multiplied by the cipher text matrix (matrix of $P_2$) giving us an intermediary plain text matrix which when subjected to modulo operation generates the final plain text matrix. We obtain the original plain text from this plain text matrix.

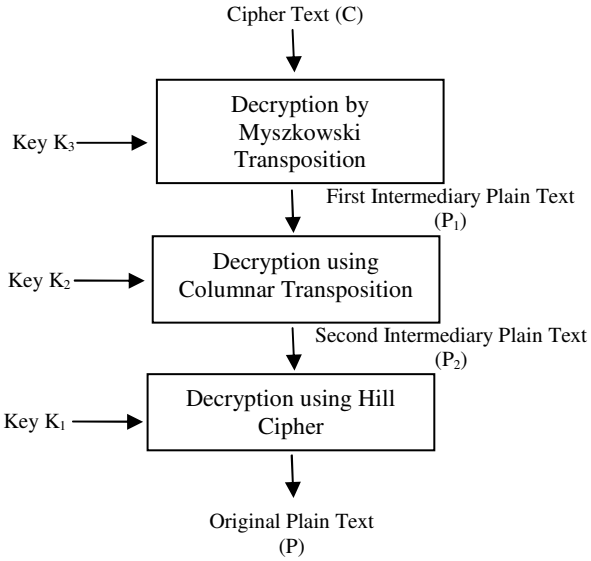


Fig 3: Proposed Decryption Steps

## IV. EXPERIMENTAL ANALYSIS

A. *Test Case 1*

| | |
|---|---|
| Plain Text (P) | CRYPTOGRAPHYANDNETWORKSECURITY |
| Keyword ($K_1$) | HVER |
| Key2 ($K_2$) | 431562 |
| Key3($K_3$) | 132412 |

Table 2

*Encryption*

STEP 1: In the first step, we apply hill cipher to the original text (P) to obtain the first intermediary cipher text ($C_1$). The first intermediary cipher text we obtain is

$C_1$ = HLDNLCJBDVHUNNIZLBGORECKSKBWNQ


© 2015, IJCSE All Rights Reserved

STEP 2: Applying Columnar Transposition on the first intermediary cipher text ($C_1$). $C_1$ is written out row-wise in Table3.

| 4 | 3 | 1 | 5 | 6 | 2 |
|---|---|---|---|---|---|
| H | L | D | N | L | C |
| J | B | D | V | H | U |
| N | N | I | Z | L | B |
| G | O | R | E | C | K |
| S | K | B | W | N | Q |

Table 3

The text from Table3 is read out column by column, the order decided by the numbering of the columns. The second intermediary cipher text resulted after columnar transposition is

$C_2$ = DDIRBCUBKQLBNOKHJNGSNVZEWLHLCN

STEP 3**:** Now Myszkowski Transposition is applied on the second intermediary cipher text ($C_2$). $C_2$ is written out row-wise in Table4.

| 1 | 3 | 2 | 4 | 1 | 2 |
|---|---|---|---|---|---|
| D | D | I | R | B | C |
| U | B | K | Q | L | B |
| N | O | K | H | J | N |
| G | S | N | V | Z | E |
| W | L | H | L | C | N |

Table 4

The text from Table4 is read out column by column, the order decided by the numbering of the columns. If two or more columns have the same number, then the text is transcribed left to right. The final cipher text (C) we obtain after Myszkowski transposition is

C = DBULNJGZWCICKBKNNEHNDBSOLRQHVL

*Decryption*

STEP 1**:** The decryption process is the reverse of encryption. In the first step, the first intermediary plain text is read out by applying the reverse of Myszkowski transposition using the key $K_3$.

| 1 | 3 | 2 | 4 | 1 | 2 |
|---|---|---|---|---|---|
| D | D | I | R | B | C |
| U | B | K | Q | L | B |
| N | O | K | H | J | N |
| G | S | N | V | Z | E |
| W | L | H | L | C | N |

Table 5

For unique column numbers, the characters are written downwards on Table 5 but for the repeating column numbers, the characters are written from left to right. The matrix, thus obtained, is read from left to right.

The first intermediary plain text obtained is

$P_1$ = DDIRBCUBKQLBNOKHJNGSNVZEWLHLCN

STEP 2: In the next step, the second intermediary plain text is read out by applying the reverse of columnar transposition using the key $K_2$. The second intermediary plain text ($P_2$) was written out column by column on Table 6 depending upon key $K_2$ and read out row-wise.

| 4 | 3 | 1 | 5 | 6 | 2 |
|---|---|---|---|---|---|
| H | L | D | N | L | C |
| J | B | D | V | H | U |
| N | N | I | Z | L | B |
| G | O | R | E | C | K |
| S | K | B | W | N | Q |

Table 6

The second intermediary plain text ($P_2$) we obtain is

$P_2$ = HLDNLCJBDVHUNNIZLBGORECKSKBWNQ

STEP 3**:** In this step, the second intermediary plain text ($P_2$) is subjected to hill cipher analysis to obtain the original text (P).

The plain text (P) obtained is

P = CRYPTOGRAPHYANDNETWORKSECURITY

B. *Test Case 2*

| Plain Text (P) | THEQUICKBROWNFOXJUMPEDOVER |
|---|---|
| Keyword (K1) | HMSJYDITR |
| Key2 | 214536 |
| Key3 | 341321 |

Table 7

*Encryption*

STEP 1: In the first step, the hill cipher is applied to the original text to obtain the first intermediary cipher text ($C_1$).

The first intermediary cipher text we obtain is

$C_1$ = DRPCYUWBPHJWNTVFPTYMHLGJ

STEP 2: Applying Columnar Transposition on the first intermediary cipher text ($C_1$). $C_1$ is written out row-wise in Table 8.

| 2 | 1 | 4 | 5 | 3 | 6 |
|---|---|---|---|---|---|
| D | R | P | C | Y | U |
| W | B | P | H | J | W |
| N | T | V | F | P | T |
| Y | M | H | L | G | J |

Table 8

The text from Table8 is read out column by column, the order decided by the numbering of the columns. The second intermediary cipher text resulted after columnar transposition is

$C_2$ = RBTMDWNYYJPGPPVHCHFLUWTJ


© 2015, IJCSE All Rights Reserved

STEP 3: Now Myszkowski Transposition is applied on the second intermediary cipher text ($C_2$). $C_2$ is written out row-wise in Table 9.

| 3 | 4 | 1 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| R | B | T | M | D | W |
| N | Y | Y | J | P | G |
| P | P | V | H | C | H |
| F | L | U | W | T | J |

Table 9

The text from Table 9 is read out column by column, the order decided by the numbering of the columns. If two or more columns have the same number, then the text is transcribed left to right. The final cipher text (C) we obtain after Myszkowski transposition is
C = TWYGVHUJDPCTRMNJPHFWBYPL

*Decryption*
STEP 1: The decryption process is the reverse of encryption. In the first step, the first intermediary plain text is read out by applying the reverse of Myszkowski transposition using the key $K_3$.

| 3 | 4 | 1 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| R | B | T | M | D | W |
| N | Y | Y | J | P | G |
| P | P | V | H | C | H |
| F | L | U | W | T | J |

Table 10

For unique column numbers, the characters are written downwards on Table 10 but for the repeating column numbers, the characters are written from left to right. The matrix, thus obtained, is read from left to right.
The first intermediary plain text obtained is
$P_1$ = RBTMDWNYYJPGPPVHCHFLUWTJ

STEP 2**:** In the next step, the second intermediary plain text is read out by applying the reverse of columnar transposition using the key $K_2$. The second intermediary plain text ($P_2$) was written out column by column on Table 11 depending upon key $K_2$ and read out row-wise.

| 2 | 1 | 4 | 5 | 3 | 6 |
|---|---|---|---|---|---|
| D | R | P | C | Y | U |
| W | B | P | H | J | W |
| N | T | V | F | P | T |
| Y | M | H | L | G | J |

Table 11

The second intermediary plain text ($P_2$) we obtain is
$P_2$ = DRPCYUWBPHJWNTVFPTYMHLGJ

STEP 3: In this step, the second intermediary plain text ($P_2$) is subjected to hill cipher analysis to obtain the original text (P).
The plain text (P) obtained is
P = THEQUICKBROWNFOXJUMPEDOVER

## V. COMPARISON WITH TRADITIONAL HILL CIPHER

Hill cipher was certainly not highly secure. Known-plaintext attack exploited the drawbacks of this cipher. Low security was the reason for the failure of hill cipher. The proposed algorithm will have a higher time and space complexity due to of introduction of columnar and Myszkowski transposition on traditional hill cipher but the level of security achieved in the modified system is higher compared to the traditional hill cipher making cryptanalysis [14] difficult.

Further, this enhancement will provide resistance to attacks on hill cipher. With the plain text subjected to hill cipher, there would be single level encryption and the encrypted text will be obtained after one substitution step. Introducing Columnar and Myszkowski transposition on keyword cipher will provide another two level encryption.

## VI. CONCLUSION AND FUTURE WORK

Hill cipher is a form of polygraphic substitution. It is unreliable as it is susceptible to cryptanalysis. As a result, hill cipher is barely put into use. In this paper, a simple but secure approach to enhance the security of hill cipher is suggested. Hill cipher has been subjected to columnar transposition and Myszkowski transposition to improve its resistance. In the first step, hill cipher is subjected to columnar transposition followed by Myszkowski transposition. The plain text is put to three levels of transposition and substitution which makes it difficult to cryptanalyze. Enhancing the security of the hill cipher will allow its more frequent use. Further, the complexity of this approach is much less and can be implemented easily.

As a part of future work, different transposition techniques could be applied to hill cipher to enhance its security. Algorithms need to be employed to enhance the time and space complexity of the system. Further, authors in [8] [9] [10] [11] [12] can introduce columnar and Myszkowski transposition on the cipher text generated by their proposed techniques.


© 2015, IJCSE All Rights Reserved

**REFERENCES**

[1] Behrouz A. Forouzan, "Cryptography and Network Security" special Indian Edition 2007, Tata McGraw- Hill Publishing Company Limited, New Delhi

[2] Ayushi, "A Symmetric Key Cryptographic Algorithm" International Journal of Computer Applications (0975 8887) Volume 1 – No. 15

[3] Atul Kahate, "Cryptography and Network Security", 2nd Edition

[4] Panduranga H T, Naveen Kumar S K. "Advanced Partial Image Encryption using Two-Stage Hill Cipher Technique", International Journal of Computer Applications (0975 – 8887) Volume 60– No.16, December 2012

[5] Yuri Borissov and Moon Ho Lee.: Bounds on Key Appearance Equivocation for Substitution Ciphers. IEEE Transactions on Information Theory Vol. 53, No.6, pp. 2294-2296 (2007).

[6] Malay B. Pramanik, "Implementation of Cryptography Technique using Columnar Transposition", International Journal of Computer Applications (0975 – 8887) Second National Conference on Recent Trends in Information Security, GHRCE, Nagpur, India, Jan-2014

[7] An article on Myszkowski Transposition: cryptospecs.googlecode.com/svn/trunk/classical/specs/myszkowski.pdf

[8] Shahrokh Saeednia, "How to Make Hill cipher Secure," Cryptologia 24:4, pp. 353-360, Oct 2000.

[9] Chefranov, A. G., "Secure Hill Cipher Modification," Proc. Of the First International Conference on Security of Information and Network (SIN2007) 7-10 May 2007, Gazimagusa (TRNC) North Cyprus, Elci, A., Ors, B., and Preneel, B (Eds) Trafford Publishing, Canada, 2008: pp 34-37, 2007.

[10] P. L. Sharma, M. Rehan, "On Security of Hill Cipher using Finite Fields", International Journal of Computer Applications (0975 – 8887) Volume 71– No.4, May 2013

[11] Kondwani Magamba, Solomon Kadaleka, Ansley Kasambara, "Variable-length Hill Cipher with MDS Key Matrix", International Journal of Computer Applications (0975 – 8887) Volume 57– No.13, November 2012

[12] Neha Sharma, Sachin Chirgaiya, "A Novel Approach to Hill Cipher", International Journal of Computer Applications (0975 – 8887) Volume 108 – No. 11, December 2014

[13] Gary C. Kessler, "An Overview of Cryptography 2014" - http://www.garykessler.net/library/crypto.html

[14] Andrew S Tanenbaum, "Computer Networks", 4th Edition

© 2015, IJCSE All Rights Reserved 