ISSN:0975-9646

Extended Hill Cipher Decryption by Using Transposed Interweaved Shifting

Divya Rathi, Parmanand Astya

Computer Science and Engg. Department, Mahamaya Technical University
MIET, Meerut India

Abstract - This paper is discussed about the strength of extended cipher due to non-linear transformation of interweave transposition and shifting operations. The impact of number of iterations on the avalanche effect is investigated. During encryption process the interweaving of the resulting plaintext, at each stage of the iteration, and the multiplication with the key matrix followed by transposition and shifting leads to confusion and diffusion. While decryption of the cipher text obtained after encryption process makes the use of reverse shifting and inverse transposed interweaving . From the cryptanalysis performed in this investigation, we have found that the cipher is a strong one. Here we propose Hill cipher modifications using Transposed Interweaved Shifting with significantly less computational complexity. The proposed modifications decrease encryption time while keeping the strength of the ciphers . It has been found that the extended algorithm takes less execution time when compared with DES and is more efficient in terms of execution.

Keywords: Interweaving, inverse interweaving, Transposed Interweaving, inverse modular arithmetic, Encryption, Decryption, Reverse Transposed interweaving

1. INTRODUCTION

Encryption is the process of converting paintext into some unreadable form. This helps in protecting the privacy while sending the data from sender to receiver. Decryption is the process of converting encrypted data back into its original form called plaintext, so that it is easily understood. Decryption is done by using the reverse algorithm as used in encryption with the inverse key K^{-1} ,which is generated by using the concept of modular arithmetic such that $K*K^{-1}$ = I(Identity matrix), that provides authentication, confidentiality and non-repudiation. Decryption is just the reverse process of encryption. Encryption is performed on plaintext at the sending end and Decryption is performed on cipher text at the receiving end. Secured communication is one which is characterized by the feature that the sender may be able to send message to receiver by preventing the eaves dropper from getting the message contents [5]. The basic building blocks of all encryption and decryption techniques are substitution and Transposition.[5, 6, 7].A substitution technique is one in which the plaintext characters of the original message are replaced by other characters. Many substitution ciphers are available practically [5]. Hill cipher is a multi-letter cipher developed by Lester Hill in 1929 [5].The Hill cipher takes m successive plaintext characters and substitutes for them m cipher text characters. Conventional Hill cipher is described as follows : C= KP mod 26, where C and P are column vectors representing the plaintext and cipher text and K is the encryption key, represented in matrix form. The same decryption process is formulated as : P= K^{-1}C mod 26. The Hill cipher has been modified by involving Interweaving and Iteration techniques[1]. Another variation to Hill cipher involves the multiplication of plaintext matrix with key matrix and confusion effect has been created by using X-OR operations between plaintext and key matrices [2]. One more block cipher design shows the use of key on one side and key inverse on other side.[3]. Similar to Hill cipher, the present cipher treats the plaintext and key values in the form of matrices. The effort of this cipher is to make cryptanalysis more difficult and making the cipher more strong. In the Hill cipher[1], cipher text C is obtained by multiplication of a plaintext vector P by a key matrix, K, i.e., by a linear transformation.

Encryption is given by:

$$C = KP(\text{mod } N), \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Decryption is given by:

$$P = K^{-1} C(\text{mod } N), \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

where K is the invertible key, N>1. It can be broken by known plaintext-cipher text attack due to its linearity. There are cryptosystems [3, 4] which have been developed in order to modify the Hill cipher to achieve higher security. In scuh cryptosystems, the Hill cipher is modified by including interweaving and iteration. They have significant avalanche effect and are supposed to resist cryptanalytic attacks. Strength of the ciphers is supposed to come from the nonlinearity of the N times applied matrix multiplication followed by interweaving as it is mentioned explicitly or implicitly in [6, 7]. In the present paper, we show that strength of the cipher modifications using interweaving [6] is due to non-linear transformation generated from transposed interweaving and circular shifting, used in investigating the impact of number of iterations, transposition and shifting on the avalanche effect, and propose generalizations of the ciphers from [6]. Then we present two new Hill cipher modifications which use bit-level permutations by interweaved transposition and only 3 iterations during shifting process .We show that in the case of performing a bit-level permutation that swaps arbitrary selected bits, even two bits, a substantial avalanche effect is achieved. The rest of the paper is organized as follows. First, a review of two Hill cipher modifications is given. Next, investigation of the number of iterations, experimental analysis and results of taking different number of iterations are presented. Then, two ciphers, row shifting Hill cipher and interweaved transposed Hill cipher are proposed simultaneously and their statistical analysis is conducted and discussed. Finally, we conclude the study.

2. Implemented Cipher Description

We introduced Transposed [1] and row shifting Hill cipher. It first makes State matrix from the interweaved cipher and then finally shifts the row of State matrix circularly left, instead of plaintext characters to generate the Cipher text. Also the introduction of transposition (arbitrary permutation) on interweaved matrix cipher uses an arbitrary permutation , not known to an opponent and shared between the two communication parties, instead of a fixed permutation (interweaving).

However, the additional steps of the extended technique are:

a. Transposed State, that is a vector of the length 4X4 , varied from intermediate cipher size which is same as P (i.e., L = nx14) with integer components from {1,…,L}. All values from 1 to L are represented in permutation in transposed interweaved order (in figure 4).

b. Number of iterations in shifting algorithm m, is considered as 3 instead of 16.

In the ciphers, during the case of shifting operation, cipher text C is defined as follows:

C= S_shlcr().

Transposed State Formation and Shift Rows are applied on the above generated intermediate cipher. Transposed State Formation allows the formation of a 4X4 matrix from the above generated 8X2 intermediate cipher matrix, where the transpose of first two rows of the previous matrix forms the first column of the current matrix and the next two rows will make the second column of the current matrix in the same fashion and so on . In shifting process the first row of the matrix is not altered, second row is shifted left circularly by one value, third row is shifted left circularly by two values and the last fourth row is shifted left circularly by three values respectively

3. Extended Hill Cipher Decryption

Hill cipher modifications by using transposed interweaving (transposition of the binary bits of the plaintext letters) and shifting has been implemented in paper [1] . The corresponding decryption process is followed by the steps given below:

Input:

The ciphertext of 2n 7-bit ASCII characters:

$P= [P_{i,j}]$, i = 1 to n, j=1 to 2…………

and a key matrix K^{-1}, such that each key matrix entry is less than 128 used in Hill Cipher Modification interweaving [5]:

a. Steps for Decryption

1)Reverse Transposed Interweaved Shifting

a) Reverse **S_shlcr()**

b) Reverse T**S_formation()**

2) Reverse Encryption Algorithm

3) Inverse interweave

4) Write P

b. Reverse Transposed Interweaved Shifting

Reverse Transposed State Formation and Reverse Shift Rows are the two steps that are performed in first step of the decryption algorithm. The function Reverse **S_shlcr()** generates a 4X4 ASCII value matrix from the cipher text obtained during encryption process where first row of the matrix is not altered and the second row is shifted right circularly by one value, third row is shifted right circularly by two values and the fourth row is shifted right circularly by three values in this matrix. Now State matrix is obtained. Then the Reverse T**S_formation()** operation is applied on this State matrix where the transposition of first column of the state matrix forms the first two rows of the intermediate cipher, transposition of second column of the state matrix forms the next two rows of the intermediate cipher and so on until an intermediate cioher matrix of order 8X2 is obtained.

c. Algorithm for Decryption

On this intermediate cipher text, represented by C, decryption algorithm is performed. The steps of decryption are as follows:

```
1) read n, N, K, P;
2) $C = KP^N$ mod 128;
2) $P^0 = C$;
3) for i = N to 1
{
$P^i = K^{-1} P^{i-1}$ mod 128;
 Reverse interweave();
}
4) Write P;
```

d) Algorithm for Reverse interweave (C):

1. Convert C into a binary nX14 matrix:

$$B = \begin{bmatrix} b_{1,1} & \cdots & b_{1,14} \\ \vdots & & \vdots \\ b_{n,1} & \cdots & b_{n,14} \end{bmatrix} \qquad (3)$$

2. Rotate circular downward the jth column of B to get new

$$\text{column as} \begin{bmatrix} b_{2,j} \\ b_{3,j} \\ \vdots \\ b_{n,j} \\ b_{1,j} \end{bmatrix} \text{where } j = 1,3,5...$$

Similarly, rotate circular rightward the j^{th} row of B where j = 2,4,6,….

4. Construct P from B using first 7 bits of j^{th} row for $P_{j,1}$ and last 7 bits for $P_{j,2}$, j = 1,2,…,n

In the implementation of Extended hill cipher algorithm[1], transposed interweaving and row wise shifting are two types of the bit-level permutation which makes total transformation non-linear that defines strength of these ciphers. The process of decryption is defined in the figure given below.

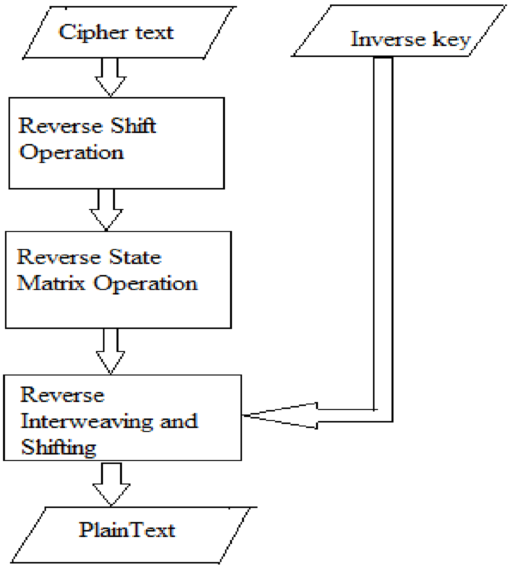

Cipher text
Inverse key
Reverse Shift Operation
Reverse State Matrix Operation
Reverse Interweaving and Shifting
PlainText

Fig. 1: flowchart for decryption of extended hill cipher algorithm by using transposed interweaved shifting

4. Avalanche Effect

The plaintext given in (1) can be represented in its binary form as

1010100110110011010001101111111001
0111100000010000011011011100100110
010111001011101110111011011101001
1001010100000. (4)

On changing the 9th character from l to m, the modified plaintext (in its binary representation) assumes the form

1010100110110111010001101111111001011
110000010000011011011100100110010111
001011101110111011011101001100101010
0000. (5)

It may be noted that the plaintexts given in Equations (4) and (5) differ by exactly one bit. The cipher text corresponding to the plaintext given in equation (4) is

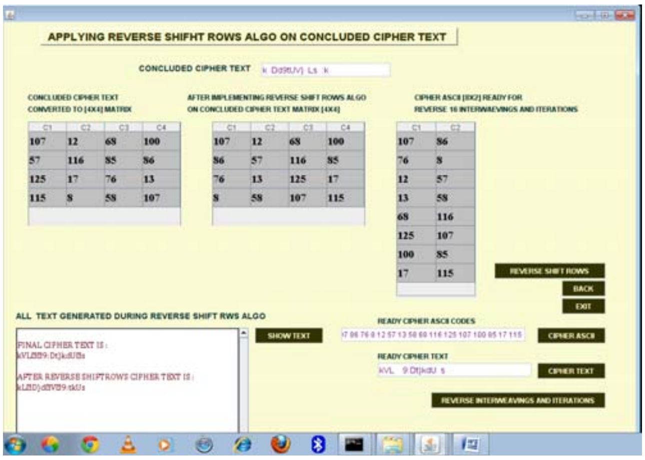
11100101100100011100010001110001000010
01010000000111010100010001000001101000
100110001010001000010010010011100011. (6)

The cipher text pertaining to the plaintext given in equation (5) can b e obtained as

000000101000100001110001000001111101000
010011000111110101111100001000010000110
00101111000110111111000000111100101. (7)

If an attacker applies C [1] on inverse of Row shifting process then he gets K*P, and the key K of the algorithm may not be detected by him against known plaintext-ciphertext attack.

Following are the screenshots of the decryption program steps:


APPLYING REVERSE SHIFHT ROWS ALGO ON CONCLUDED CIPHER TEXT

CONCLUDED CIPHER TEXT: k Dd9tUVj Ls k

CONCLUDED CIPHER TEXT CONVERTED TO [4X4] MATRIX

C1	C2	C3	C4
107	12	68	100
57	116	85	86
125	17	76	13
115	8	58	107

AFTER IMPLEMENTING REVERSE SHIFT ROWS ALGO ON CONCLUDED CIPHER TEXT MATRIX [4X4]

C1	C2	C3	C4
107	12	68	100
86	57	116	85
76	13	125	17
8	58	107	115

CIPHER ASCII [8X2] READY FOR REVERSE 16 INTERWAEVINGS AND ITERATIONS

C1	C2
107	86
76	8
12	57
13	58
68	116
125	107
100	85
17	115

ALL TEXT GENERATED DURING REVERSE SHIFT RWS ALGO

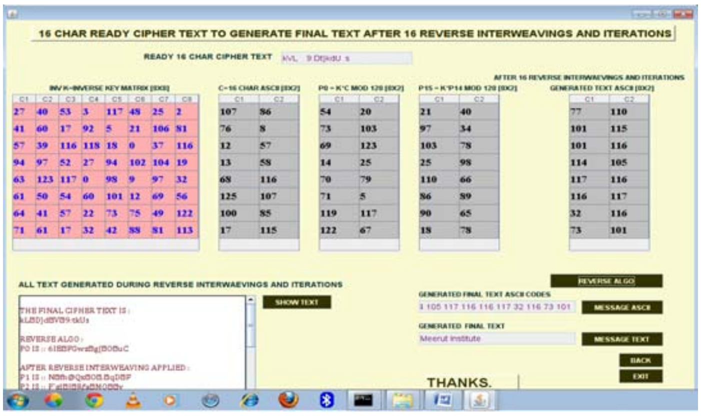
FINAL CIPHER TEXT IS :
kVL8B9:DtjkdUBs

AFTER REVERSE SHIFTROWS CIPHER TEXT IS :
kLEID)d8VB9:tkUs

READY CIPHER ASCII CODES: 7 86 76 8 12 57 13 58 68 116 125 107 100 85 17 115

READY CIPHER TEXT: kVL 9 Dt|kdU s

Fig 2: Reverse Shift Row operation and Reverse state matrix formation


16 CHAR READY CIPHER TEXT TO GENERATE FINAL TEXT AFTER 16 REVERSE INTERWEAVINGS AND ITERATIONS

READY 16 CHAR CIPHER TEXT: kVL 9 Dt|kdU s

INV K=INVERSE KEY MATRIX [8X8]

C1	C2	C3	C4	C5	C6	C7	C8
27	40	53	3	117	48	25	2
41	60	17	92	5	21	106	81
57	39	116	118	18	0	37	116
94	97	52	27	94	102	104	19
63	123	117	0	98	9	97	32
61	50	54	60	101	12	69	56
64	41	57	22	73	75	49	122
71	61	17	32	42	88	81	113

C=16 CHAR ASCII [8X2]

C1	C2
107	86
76	8
12	57
13	58
68	116
125	107
100	85
17	115

P0 = K*C MOD 128 [8X2]

C1	C2
54	20
73	103
69	123
14	25
70	79
71	5
119	117
122	67

P15 = K*P14 MOD 128 [8X2]

C1	C2
21	40
97	34
103	78
25	98
110	66
86	89
90	65
18	78

AFTER 16 REVERSE INTERWAEVINGS AND ITERATIONS GENERATED TEXT ASCII [8X2]

C1	C2
77	110
101	115
101	116
114	105
117	116
116	117
32	116
73	101

ALL TEXT GENERATED DURING REVERSE INTERWAEVINGS AND ITERATIONS

THE FINAL CIPHER TEXT IS :
kLEID)d8VB9:tkUs

REVERSE ALGO :
P0 IS :: 6IEEFGwzBg{BOBuC

AFTER REVERSE INTERWEAVING APPLIED :
P1 IS :: N8fh@QxBOB.BqDBP
P2 IS :: F'alBIB8fa8M0BBv

GENERATED FINAL TEXT ASCII CODES: 1 105 117 116 116 117 32 116 73 101

GENERATED FINAL TEXT: Meerut institute

THANKS.

Fig 3: Retrieved Plaintext after reverse Interweaving and Iteration

5. Analysis And Discussions

A desirable aspect in network communication is the secured communication channel. The information that is being transmitted should be protected from both active and passive attacks [1]. The p modified cipher provides more security to the plaintext message that is being transmitted through the network from eavesdropper. The cipher requires a secured transposition factor in addition to key value. The length of the key and multiplication factor plays a very important role in providing security. Thus selecting the value for key and multiplication factor is very important to get more security without reducing the encryption speed.

The susceptibility of known plaintext-cipher text attack in hill cipher is due to its linearity. In this study, decryption process and the extended hill cipher performance are discussed by two hill cipher modification steps of transposed interweaving and row shifting on state matrix. Also bit level permutations and 16 steps of iterations are used that makes extended hill cipher more secured against any possibility of attack. It has been shown that the cipher is strengthened by the use of non-linear transformation(bit level permutation). The avalanche effect has been significantly observed and the introduction of row-wise shifting generates more confusion and diffusion to the cipher by increasing non linear independency of column vectors of transposed matrix. Statistical results of the tests for decryption process and performance of extended hill cipher are shown in the given below graphs.

A. Experimental Results:

The figure which is given below illustrates the experimental time taken to decrypt each piece of ciphertext (each is of different data loads) in seconds.

The time taken by loading the process and preparing the inversekey is ignored because it is comparatively small to processing time.

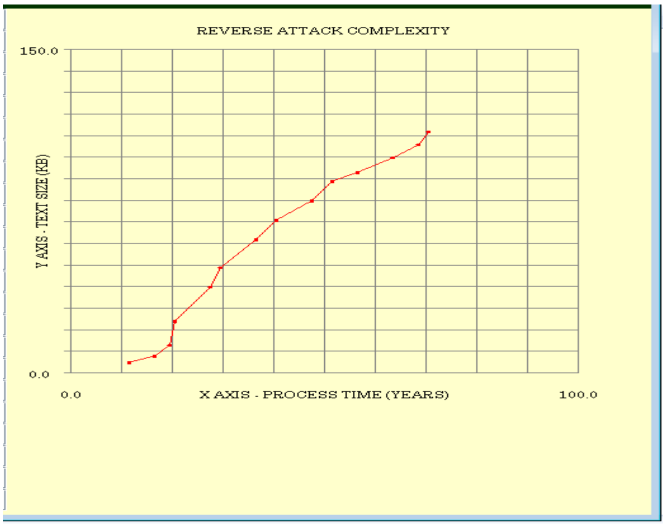


Fig 4: Process time graph for decryption of extended hill cipher algorithm

B. Comparison Result

When we compare our proposed [1] or extended hill cipher algorithm for same set of plaintext with DES then we found that Extended hill cipher algorithm take less processing time than DES. The figure which is given below illustrates that DES represented by yellow line takes more processing time than EHS as represented by green line.

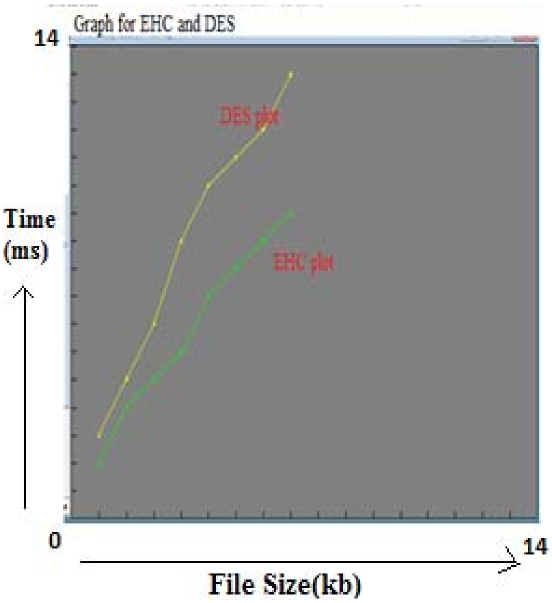


Fig 5:Graph plotting for EHS and DES

6. Conclusion

Our future work was dedicated [1] to implement the reverse algorithm for decryption process to revert back the cipher text into its plain text value. In addition to decryption, we will implement this encoding on other known algorithms to measure extended hill cipher algorithm's performance and security. The experimental results in figure as shown above proves that for an attacker attempt to decrypt a cipher, years will be required to decode the message. Hence the extended encryption and decryption algorithm is found to be more secured for exchange of messages between sender and receiver by maintaining security, integrity and confidentiality of message. The extension by interweaved transposition shifting [1] and iterations are responsible for this. When the extended implemented algorithm is compared with different algorithms, it has been found that it takes less execution time and is more efficient in terms of execution. The Hill cipher has been made more secured against the attack by using above mentioned concept. The strength of the ciphers is due to non-linear transformation used in transposition and shifting cipher. It has been observed that for number of iterations from 1 to 16 and two modified steps, avalanche effect has significant importance by introducing more confusion and diffusion in this algorithm.

REFERENCES

[1] Divya Rathi1, Parmanand Astya2 , Ankur Garg3, “Extended Hill Cipher Encryption by using Transposed Interweaved Shifting”, International Journal of Mobile & Adhoc Network |Vol 4|issue 1|Feb.2014, *http://ifrsa.org/images/ijmanvol4issue1/6%20six.pdf*

[2] A.F.A. Abidin, O.Y. Chuan and M.R.K, “A Novel Enhancement Technique of the Hill Cipher for Effective Cryptographic Purposes”, *Ariffin, Journal of Computer Science,* 7 (5): 785-789, ISSN 1549-3636© 2011 Science Publications ,2011.

[3] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, “Image Encryption Using Advanced Hill CipherAlgorithm”, *ACEEE International Journal on Signal and Image Processing* ,Vol 1, No. 1, Jan 2010.

[4] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy, “Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm” , *International Journal of Security*, Vol 1, Issue 1, 2007, pp. 14-21, 2007.

[5] Cryptography and Network Security by *William Stallings , Fourth Edition,*2005.

[6] Dr. H.K. Pathak et. al./ ,”Public key cryptosystem and a key exchange protocol using tools of non-abelian group”, *International Journal on Computer Science and Engineering,* Vol. 02, No. 04, 2010, 1029-1033.

[7] Min-Shiang-Hwang, Cheng-Chi Lee and Shiang-Feng Tzeng, ”A New Knapsack Public-Key Cryptosystem Based on Permutation Combination Algorithm”,*World Academy of Science, Engineering and Technology* 33 2009.

[8] Recommendation for Cryptographic Key Generation,NIST Special Publication,July 2011

[9] V.U.K.Sastry, Aruna Varanasi and S.Udaya Kumar, “A Modern Advanced Hill Cipher Involving XOR Operation and Permuted Key” *,A Research paper by Journal of Global Research in Computer Science*, Volume 2, No. 4, April 2011

[10] V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar, ”Advanced Hill Cipher Involving a Pair of Keys”, *International Journal of Computational Intelligence and Information Security*, Vol.2 No.1, pp 100 -108, January2011.

[11] V. Umakanta Sastry, N. Ravi Shankar, and S Durga Bhavani, “A Modified Hill Cipher Involving Interweaving and Iteration”, *International Journal of Network Security*, Vol.11, No.1,2010.

[12] V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar , “Advanced Hill Cipher Involving Permutation and Iteration”, *International Journal of Advanced Research in Computer Science*, Vol.1, No.4, pp. 141- 145, Nov-Dec. 2010.

[13] Bruce S. ,*Applied Cryptography*, John Wiley and Sons, 2nd Edition, 1996.