On Security of Hill Cipher using Finite Fields

P. L. Sharma
Department of Mathmatics
Summer Hill, Shimla

M. Rehan
Department of Mathmatics
Summer Hill, Shimla

ABSTRACT

Hill cipher in cryptography is a symmetric key substitution algorithm, which is vulnerable to known plaintext attack. The present paper provides two fold securities to the existing Hill cipher by using the elements of finite fields and logical operator.

Keywords

Plain Text; Symmetric Key; Hill Cipher; Finite Field; Logical Operator.

MSC : 11T71, 94A60, 68P25.

1. INTRODUCTION

The security of information to maintain its confidentiality, integrity and availability has become a major issue today. Cryptography is a cornerstone of the modern electronic security technologies used today to protect valuable information resources on intranets, extranets, and the internet [1, 2]. It is the study of techniques and applications of protecting the integrity and authenticity of information sent through insecure channels. Various techniques from different areas of mathematics like number theory, matrix analysis, finite fields [3], logical operators [4] etc. are used in building and analysing ciphers.

The Hill cipher in cryptography is a classical symmetric cipher based on matrix transformation. It was invented by Lester S. Hill in 1929 [5]. He extended this work in [6]. The main advantages of Hill cipher includes its frequency analysis, high speed, high throughput and the simplicity due to the fact that it uses matrix multiplication and inversion for encryption / decryption. However it succumbs to the known plaintext attack [7, 8]. In Hill cipher for decryption to be possible, the key matrix should be invertible. According to Overbay [9] the key space of Hill cipher is $GL(n, Z_m)$, the group of $n \times n$ matrices that are invertible over Z_m, where Z_m is ring of integers modulo m [10].

Several researchers have contributed to improve the security of Hill Cipher. Saeednia [11] tried to make Hill cipher secure by using the dynamic key matrix obtained by random permutations of columns and rows of the master key matrix. Chefranov [12] proposed a modification to [11] which is similar to Hill cipher permutation method but it uses a pseudo-random permutation generator. The number of dynamic keys is same as taken in [11]. Ismail et al. [13] in their technique for repairing Hill cipher introduced an initial vector that multiplies each row of current key matrix to form a different key for each block encryption. Adi et al. [14] modified the Hill cipher based on circulant matrices. In their cryptosystem, they have used a prime circulant matrix.

We give an algorithm which increases the security of Hill cipher. The proposed algorithm along with illustration involves the encryption and decryption of plaintext by making the use of elements of finite fields and logical $XNOR$ operator.

2. ALGORITHM OF PROPOSED CRYPTOSYSTEM

Two different keys are used in the proposed algorithm. The first key is taken as a non singular matrix and the second key is obtained with the help of elements of finite fields. The elements of finite fields are used in binary & polynomial form [2] during encryption and decryption of the message.

ENCRYPTION:

1. Sender and receiver shares the secret key K_1, where K_1 is $(n-1) \times (n-1)$ non-singular matrix and n is a positive integer.
2. The sender converts the plaintext into pre-assigned numerical values and calculates $S_1 = K_1 P (mod\ 2^n - 1)$; S_1 is the first cipher text, P is the plain text.
3. Then sender converts S_1 into binary string of n-bits which gives matrix M & choose a random matrix A of order $(n-1) \times (n-1)$.
4. Sender performs $XNOR$ operation with randomly selected rows/columns of A with each row of matrix M and gets a matrix M_{XNOR}.
5. Now the sender converts the entries of M_{XNOR} into the elements of $GF(2^n)$ & multiply each entry with g^n and calculates K_2,whose entries are 1 if g has the power greater than $2^n - 1$ otherwise 0 and shares it with receiver.
6. He then reduces the powers of the entries to $mod\ (2^n - 1)$ and gets the matrix M_4.
7. After writing it into binary form, he converts the same in numerical values and then into text to get the final cipher text S_2.

DECRYPTION:

1. The receiver receives the message. After changing it into numerical values, he converts them in binary elements of n-bits and then into elements of $GF(2^n)$ to get D_1.
2. Receiver then multiplies the entries of D_1 with g^{2^n-1} which represents 1 in the corresponding key matrix K_2.
3. Receiver then multiplies each entry with g^{-n} & converts them in binary elements of n-bits.
4. Receiver recognizes the rows/columns of matrix randomly chosen by the sender and he converts them in binary elements of n-bits to perform $XNOR$ with each row of the matrix obtained in step 3.
5. Then receiver converts the entries in numerical values to obtain S_1.
6. He then finds $P = K_1^{-1} S_1 (mod\ (2^n - 1))$.
7. Then the receiver converts the entries of P in text to get the plaintext.

Let the letters of the alphabets and some more symbols be associated with integers as follows

Table 1

Numerical values for alphabets and some symbols used in the paper

@	A	B	C	D	E	F	G
0	1	2	3	4	5	6	7
H	I	J	K	L	M	N	O
8	9	10	11	12	13	14	15
P	Q	R	S	T	U	V	W
16	17	18	19	20	21	22	23
X	Y	Z	[	\	]	^	
24	25	26	27	28	29	30	

3. ILLUSTRATION

Let us consider the message which is to be sent on the insecure channel is **[EVARISTEGALOIS]**.

ENCRYPTION:

Step1. Sender considers the 4×4 non-singular key matrix K_1 & shares it with the receiver.

$$K_1 = \begin{bmatrix} 2 & 1 & 2 & 1 \\ 3 & 5 & 2 & 2 \\ 5 & 1 & 3 & 1 \\ 3 & 1 & 3 & 2 \end{bmatrix}$$

Step 2. Sender converts the above plain text into numerical values using Table 1 which gives,

$$P = \begin{bmatrix} 27 & 5 & 22 & 1 \\ 18 & 9 & 19 & 20 \\ 5 & 7 & 1 & 12 \\ 15 & 9 & 19 & 29 \end{bmatrix}$$

Therefore,

$$K_1P = \begin{bmatrix} 2 & 1 & 2 & 1 \\ 3 & 5 & 2 & 2 \\ 5 & 1 & 3 & 1 \\ 3 & 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 27 & 5 & 22 & 1 \\ 18 & 9 & 19 & 20 \\ 5 & 7 & 1 & 12 \\ 15 & 9 & 19 & 29 \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 11 & 22 & 13 \\ 25 & 30 & 15 & 30 \\ 28 & 2 & 27 & 28 \\ 20 & 1 & 2 & 24 \end{bmatrix} = S_1(say)$$

Step 3. Sender converts the above numerical values into 5-bit binary string and therefore S_1 gives

$$M = \begin{bmatrix} 00100 & 01011 & 10110 & 01101 \\ 11001 & 11110 & 01111 & 11110 \\ 11100 & 00010 & 11011 & 11100 \\ 10100 & 00001 & 00010 & 11000 \end{bmatrix}.$$

Now sender randomly choses 4×4 matrix A as follows

$$A = \begin{bmatrix} 2 & 5 & 2 & 3 \\ 2 & 4 & 2 & 6 \\ 3 & 3 & 4 & 6 \\ 2 & 3 & 1 & 3 \end{bmatrix}.$$

Step 4. Sender now selects the rows/columns C_1, C_2, R_2, R_3 from the matrix A at random to perform logical $XNOR$ operation with each row of matrix M. Sender converts the elements of C_1 into 5-bit binary number & performs logical operator with first row of matrix M

00010000100001100010

$XNOR$

00100010111011001101

which gives the first row of matrix M_{XNOR}

11001101100101010000.

Similarly C_2, R_2, R_3 are converted into binary numbers and logical operator $XNOR$ is performed with second, third and fourth rows of matrix M respectively.

Therefore,

00101001000001100011

$XNOR$

11001111100111111110

gives

00011001011001100010

as IInd row of matrix M_{XNOR} and

00010001000001000110

$XNOR$

11100000101101111100

gives

00001110010011000101

as the IIIrd row of matrix M_{XNOR} and

00011000110010000110

$XNOR$

10100000010001011000

makes the IVth row of matrix M_{XNOR} as

01000111011100100001.

Hence the matrix M_{XNOR} is

$$M_{XNOR} = \begin{bmatrix} 11001 & 10110 & 01010 & 10000 \\ 00011 & 00101 & 10011 & 00010 \\ 00001 & 11001 & 00110 & 00101 \\ 01000 & 11101 & 11001 & 00001 \end{bmatrix}.$$

Step 5. Sender converts the above entries into the elements of $GF(2^5)$ in their basis form such that $(g^5 + g^2 + 1) = 0$, we have

$$M_2 = \begin{bmatrix} g^{25} & g^{28} & g^6 & g^4 \\ g^{18} & g^5 & g^{17} & g^1 \\ g^0 & g^{25} & g^{19} & g^5 \\ g^3 & g^{14} & g^{25} & g^0 \end{bmatrix}$$

Multiply the above entries by g^5 . Therefore, M_2 becomes

$$M_3 = \begin{bmatrix} g^{30} & g^{33} & g^{11} & g^{9} \\ g^{23} & g^{10} & g^{22} & g^{6} \\ g^{5} & g^{30} & g^{24} & g^{10} \\ g^{8} & g^{19} & g^{30} & g^{5} \end{bmatrix}$$

and the key matrix

$$K_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

is chosen in such a way that if power of g in M_3 is less than 31, the entry in the key matrix is taken 0 otherwise 1.

Step 6. M_3 is reduced to mod 31 and hence it becomes

$$M_4 = \begin{bmatrix} g^{30} & g^{2} & g^{11} & g^{9} \\ g^{23} & g^{10} & g^{22} & g^{6} \\ g^{5} & g^{30} & g^{24} & g^{10} \\ g^{8} & g^{19} & g^{30} & g^{5} \end{bmatrix}$$

Step 7. The elements of cipher text matrix M_4 are converted in binary elements as follows,

$$S_2 = \begin{bmatrix} 10010 & 00100 & 00111 & 11010 \\ 01111 & 10001 & 10101 & 01010 \\ 00101 & 10010 & 11110 & 10001 \\ 01101 & 00110 & 10010 & 00101 \end{bmatrix}$$

These entries of S_2 are then converted into numerical values, which gives

$$S_3 = \begin{bmatrix} 18 & 4 & 7 & 26 \\ 15 & 17 & 21 & 10 \\ 5 & 18 & 30 & 17 \\ 13 & 6 & 18 & 5 \end{bmatrix}$$

and numerical values are converted into text using the Table 1.

So the cipher text is **RDGZOQUJER^QMFRE.**

The cipher text is sent to the receiver through public channel.

DECRYPTION:

Step 1. The receiver receives the message. He converts the message in numerical values using Table 1 and after converting numerical values in binary elements of 5-bits, he writes them in the form of a matrix, which gives

$$S_2 = \begin{bmatrix} 10010 & 00100 & 00111 & 11010 \\ 01111 & 10001 & 10101 & 01010 \\ 00101 & 10010 & 11110 & 10001 \\ 01101 & 00110 & 10010 & 00101 \end{bmatrix}.$$

Then he converts these entries in the elements of $GF(2^5)$ and S_2 becomes

$$D_1 = \begin{bmatrix} g^{30} & g^{2} & g^{11} & g^{9} \\ g^{23} & g^{10} & g^{22} & g^{6} \\ g^{5} & g^{30} & g^{24} & g^{10} \\ g^{8} & g^{19} & g^{30} & g^{5} \end{bmatrix}.$$

Step 2. Receiver multiplies those entries of D_1 with g^{31} which represents 1 in the corresponding key matrix K_2. Therefore transformed matrix is

$$D_2 = \begin{bmatrix} g^{30} & g^{33} & g^{11} & g^{9} \\ g^{23} & g^{10} & g^{22} & g^{6} \\ g^{5} & g^{30} & g^{24} & g^{10} \\ g^{8} & g^{19} & g^{30} & g^{5} \end{bmatrix}.$$

Step 3. Now the receiver multiply D_2 with g^{-5} and obtain

$$D_3 = \begin{bmatrix} g^{25} & g^{28} & g^{6} & g^{4} \\ g^{18} & g^{5} & g^{17} & g^{1} \\ g^{0} & g^{25} & g^{19} & g^{5} \\ g^{3} & g^{14} & g^{25} & g^{0} \end{bmatrix}.$$

Therefore the binary representation of D_3 is

$$D_4 = \begin{bmatrix} 11001 & 10110 & 01010 & 10000 \\ 00011 & 00101 & 10011 & 00010 \\ 00001 & 11001 & 00110 & 00101 \\ 01000 & 11101 & 11001 & 00001 \end{bmatrix}.$$

Step 4. Receiver recognizes the rows /columns C_1, C_2, R_2, R_3 of the matrix A selected by the sender. He then converts its elements contained in C_1 into 5-bit binary number and performs logical operator with first row of D_4.

Therefore,

00010000100001100010

$XNOR$

11001101100101010000

which gives the first row of matrix M as

00100010111011001101.

Similarly C_2, R_2, R_3 are converted into binary string of 5-bits and logical operator $XNOR$ is performed respectively with second, third and fourth rows of matrix D_4.

Therefore,

00101001000001100011

$XNOR$

00011001011001100010

gives the IInd row of matrix M as

11001111100111111110

and

00010001000001000110

$XNOR$

00001110010011000101

gives the IIIrd row of matrix M as

11100000101101111100

and

00011000110010000110

$XNOR$

01000111011100100001

results the IVth row of matrix M as

10100000010001011000.

Hence the matrix M is

$$M = \begin{bmatrix} 00100 & 01011 & 10110 & 01101 \\ 11001 & 11110 & 01111 & 11110 \\ 11100 & 00010 & 11011 & 11100 \\ 10100 & 00001 & 00010 & 11000 \end{bmatrix}.$$

Step 5. Receiver converts these entries of M in numerical values and hence it becomes

$$S_1 = \begin{bmatrix} 4 & 11 & 22 & 13 \\ 25 & 30 & 15 & 30 \\ 28 & 2 & 27 & 28 \\ 20 & 1 & 2 & 24 \end{bmatrix}.$$

Step 6. The receiver finds $K_1^{-1}S_1\ (mod\ 31)$.
Therefore,

$K_1^{-1}S_1$

$$= \begin{bmatrix} 27 & 17 & 23 & 20 \\ 26 & 3 & 14 & 8 \\ 11 & 11 & 25 & 2 \\ 23 & 3 & 14 & 10 \end{bmatrix} \begin{bmatrix} 4 & 11 & 22 & 13 \\ 25 & 30 & 15 & 30 \\ 28 & 2 & 27 & 28 \\ 20 & 1 & 2 & 24 \end{bmatrix} (mod\ 31)$$

$$= \begin{bmatrix} 27 & 5 & 22 & 1 \\ 18 & 9 & 19 & 20 \\ 5 & 7 & 1 & 12 \\ 15 & 9 & 19 & 29 \end{bmatrix}.$$

Step 7. Receiver converts the digits in text using Table 1 and the plain text **[EVARISTEGALOIS]** is obtained.

4. CONCLUSION

The proposed cryptosystem is based on the elements of finite fields, which is an extension of the original Hill cipher. It provides security in two levels. In this cryptosystem, the second key is different for different block data which gives difficulty for adversary to break the cryptosystem. Therefore, there are least possibilities of Brute force attack. Here also, the cipher text cannot be broken with the known plain text attack as there is no direct relation between plain text and cipher text even if the key matrices are known.

5. ACKNOWLEDGMENTS

Authors acknowledge the support of UGC-SAP and are grateful to Professor R. K. Sharma, Department of Mathematics, IIT Delhi for his valuable guidance and suggestions. Authors also thank the referee for his comments to bring the paper in the present form.

.

6. REFERENCES

[1] Stallings, W. 2006. Cryptography and Network Security. Fourth Edition. Pearson.

[2] Schneier, B. 2007. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Second Edition. John Wiley& Sons.

[3] Lidl, R., and Niederreiter, H. 1997. Finite Fields. Cambridge University Press. Cambridge. Second Edition.

[4] Lakshami, G. N., Kumar, B. R., Suneetha, Ch., and Chandra Shekhar, A. 2011. A Cryptographic Scheme of Finite Fields Using Logical Operators. International Journal of Computer Applications. 31(4), p.1- 4.

[5] Hill, L.S. 1929. Cryptography in an Algebraic Alphabet. American Mathematical Monthly. 36, p. 306-312.

[6] Hill, L. S. 1931. Concerning Certain Linear Transformation Apparatus of Cryptography. American Mathematical Monthly. 38, p. 135-154.

[7] Buchmann, J.A. 2004. Introduction to Cryptography. Second Edition. Springer-Verlag. New York.

[8] Stinson, D.R. 2006. Cryptography Theory and Practice. Third Edition. Chapman & Hall/CRC.

[9] Overbey, J., Traves, W., and Wojdylo, J. 2005. On The Key Space of The Hill Cipher. Cryptologia. 29(1), p. 59-72.

[10] Koblitz, N. 1994. A Course in Number Theory and Cryptography. Springer Verlag. New York.

[11] Saeednia's, S. 2000. How to Make The Hill Cipher Secure. Cryptologia. 24, p. 353-360.

[12] Chefranov, A.G. 2007. Secure Hill Cipher Modification SHC-M. Proceedings of the First Internationl Conference on Security of Information and Networks. Trafford Publishing. Canada, p. 34-37.

[13] Ismail, I.A., Amin, M., and Diab, H. 2006. How to Repair Hill Cipher. Journal of Zhejiang University-Science A. 7(12), p. 2022-2030.

[14] Adi, N.R.K., Vishnuvardhan, B., Madhuviswanath, V., and Krishna, A.V.N. 2012. A Modified Hill Cipher Based on Circulant Matrices. Procedia Technology (Elsevier). 4, p. 114-118.