CAREER POINT UNIVERSITY HAMIRPUR

CPUH-Research Journal: **2017, *2(2),*** 45-50
ISSN (Online): 2455-6076
http://www.cpuh.in/academics/academic_journals.php

A SYMMETRIC CRYPTOSYSTEM BASED ON IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

***P. L. Sharma[1], Shabnam Sharma[2] & Arun Kumar[1]**

[1]Department of Mathematics and Statistics, Himachal Pradesh University, Shimla 171005, India
[2]Government Polytechnic Bilaspur, Himachal Pradesh
Email: plsharma1964@gmail.com

ABSTRACT: Irreducible polynomials over finite fields play an important role in cryptography. Various cryptosystems are based on the irreducible polynomials. In the present paper, we discuss a symmetric cryptosystem using irreducible polynomial of degree four over finite field GF (2).

A**MS classification: 11T71, 94A60**.

Keywords: Plain text; cipher text; irreducible polynomial; finite field.

INTRODUCTION: Secured communication of text information is prime importance across the world. Cryptography is the science which provides confidentiality, authenticity and integrity of information passing through insecure channels, see [10,11]. Although the ultimate goal of cryptography is to hide information from unauthorized individuals. Most algorithms can be broken and the information can be revealed if the attacker has enough time, desire, and resources. As a result researchers are using new techniques from different areas of mathematics like matrix analysis, finite fields [6, 23-26] etc. for the security of data during transmission. There are similar structures to matrices which are known as rhotrices. Such structures came into existence in the literature since 2003. Various researchers have used these rhotrices to develop their structures and apply the same in the field of cryptography, see [12-19].

There are various algorithms in cryptography which are used to encrypt and decrypt the data for security purposes. The Hill cipher is classical symmetric cipher invented by Lester S. Hill in 1929 [3] and extension of this work is in [4]. The main advantages of Hill cipher includes its frequency analysis, high speed, high throughput and the simplicity because it uses matrix operations but it succumbs to the known plaintext attack [5]. Hill cipher is modified by several authors. Saeednia [7] uses the dynamic key matrix while Chefranov [2] uses a pseudo-random permutation generator. Ismail et al. [5] give an initial vector to form a different key for each block encryption. Adi et al. [1] modify the Hill cipher using circulant matrices. Shastry et al. [8, 9] use the key on both sides of the plain text to modify Hill cipher. Sharma and Rehan [20, 21] modify Hill cipher using logical operator. Sharma and Sharma [22] modify Hill cipher using elements of finite field. We give an algorithm along with illustration which involves the encryption and decryption of plaintext by using irreducible polynomials over finite field $GF(2)$. In the proposed cipher, we use the following matrices and the irreducible polynomial.

Vandermonde matrix: A matrix $V(a_1, a_2, \dots, a_m)$ of order $m \times n$ having terms in each row with a geometric progression is called Vandermonde matrix and is written as

$$V = \begin{bmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \dots & a_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_m & a_m^2 & \dots & a_m^{n-1} \end{bmatrix}.$$

Coefficient matrix: Let M be a $n \times n$ matrix, then the coefficient matrix is defined as $circ(circ(row\ 1), circ(row\ 2), \dots, circ(row n))$, where $row\ 1$, $row\ 2, \dots, row\ n$ are rows of matrix M and $circ(row\ 1)$ is the circulant matrix of row 1. It is denoted by M_c.

Example: If M be a 2×2 matrix, then its coefficient matrix M_c is 4×4.

$$M = \begin{bmatrix} h_1 & h_2 \\ h_3 & h_4 \end{bmatrix},$$

$$M_c = \begin{bmatrix} h_1 & h_2 & h_3 & h_4 \\ h_2 & h_1 & h_4 & h_3 \\ h_3 & h_4 & h_1 & h_2 \\ h_4 & h_3 & h_2 & h_1 \end{bmatrix}.$$

Representation of elements in finite fields:
The finite field $\mathbb{F}_{2^4}$ has 16 elements. These elements can be represented by the following Table 1 with respect to the irreducible polynomial $f(x) = x^4 + x + 1$ over $\mathbb{F}_2$. Let $\alpha \in \mathbb{F}_{2^4}$ be a root of the irreducible polynomial $f(x)$. Therefore, $f(\alpha) = 0$. This gives, $\alpha^4 = \alpha + 1$, which is used to reduce the higher power of α.

Table 1: Representation of elements

Powers of α	Polynomial representation	Binary $\alpha^3\alpha^2\alpha^1\alpha^0$	Decimal
0	0	0 0 0 0	0
α^0	1	0 0 0 1	1
α^1	α	0 0 1 0	2
α^2	α^2	0 1 0 0	4
α^3	α^3	1 0 0 0	8
α^4	$\alpha+1$	0 0 1 1	3
α^5	$\alpha^2+\alpha$	0 1 1 0	6
α^6	$\alpha^3+\alpha^2$	1 1 0 0	12
α^7	$\alpha^3+\alpha+1$	1 0 1 1	11
α^8	α^2+1	0 1 0 1	5
α^9	$\alpha^3+\alpha$	1 0 1 0	10
α^{10}	$\alpha^2+\alpha+1$	0 1 1 1	7
α^{11}	$\alpha^3+\alpha^2+\alpha$	1 1 1 0	14
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1 1 1 1	15
α^{13}	$\alpha^3+\alpha^2+1$	1 1 0 1	13
α^{14}	α^3+1	1 0 0 1	9

ALGORITHM OF THE PROPOSED CRYPTOSYSTEM: In the proposed algorithm, we use the elements of finite field and also use irreducible polynomials over Galois field $GF(2^m)$.

ENCRYPTION:

1. Sender select a $n \times n$ Vander monde matrix M as secret key.
2. Select a $n \times n$ non singular matrix S such that $\det(S_c) = 0$.
3. He calculates key $K_1 = MSM^{-1}(mod\ p)$, where p is an irreducible polynomial of degree m over finite field $GF(2)$.

4. The sender converts the plain text into numerical values by using Table 2.
5. He then converts the numerical values into binary strings of m − bits.
6. Further, he converts $m-$ bits binary strings into polynomial form.
7. Sender calculates $C_i = (K_1 P_i + S_i^t)(mod\ p)$, where M_i is the i^{th} cipher text block, P_i is the i^{th} plain text block and S_i is the i^{th} row of Vander monde matrix . Each entry of M_i is multiplied with x^m and sender calculates K_2, whose entries are 0 if x has the power less than $2^m - 1$ otherwise 1 and shares it with the receiver.
8. Sender reduces the powers of the entries by $mod\ (2^m - 1)$ and gets the matrix S_3.
9. After writing it into binary form, he converts the same in numerical values and then in text to get the final cipher text S_4.

DECRYPTION:

1. Receiver receives the message. He converts the message into numerical values by using the Table 2.
2. He converts the numerical values into binary string of m -bits.
3. Then he converts the binary strings into the elements of $GF(2^m)$ to get S_3.
4. He then multiplies each entry of S_3 with x^{2^m-1} which represents 1 in the matrix K_2.
5. Receiver multiplies each entry with x^{-m} to obtain S_1.
6. He calculate key $K_1^{-1} = SA^{-1}S^{-1}(mod\ p)$, where p is an irreducible polynomial of degree m over finite field $GF(2)$.
7. Further, he calculates $P_i = K_1^{-1}(C_i - S_i^t)(mod p)$.
8. Then he converts the entries into binary strings to get P_i.
9. Then the receiver converts the entries of P_i into numerical values. After writing it into numerical values, he converts the same into text to get plaintext.

Table 2: Numerical values for alphabets and some symbols used in the paper.

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

ILLUSTRATION OF THE CIPHER

Let us consider the following plain text which is to be sent over an insecure channel is−**DGA.** Further, we consider the irreducible polynomial x^4+x+1 with α as its root and finite field $GF(2^4)$.

ENCRYPTION:

Step 1. Sender considers the 2× 2 Vandermonde matrix S.

$$M = \begin{bmatrix} 1 & x+1 \\ 1 & x^3+1 \end{bmatrix}, \text{ where } x+1,\ x^3+1 \in GF(2^4).$$

Step 2. Select a 2× 2 non singular matrix S whose elements are from $GF(2^4)$ as public key.

$$S = \begin{bmatrix} x & x+1 \\ x^2 & x^2+1 \end{bmatrix}.$$

Step 3. Calculate the key

$$K_1 = MSM^{-1} = \begin{bmatrix} 1 & x+1 \\ 1 & x^3+1 \end{bmatrix}\begin{bmatrix} x & x+1 \\ x^2 & x^2+1 \end{bmatrix}\begin{bmatrix} x^2+x & x^2+x+1 \\ x^3+x^2 & x^3+x^2 \end{bmatrix}(mod x^4+x+1).$$

$$= \begin{bmatrix} x^3+x^2+1 & x+1 \\ x^3+x & x^3+x \end{bmatrix}.$$

Step 4. Sender converts the first two alphabets −**D** of plaintext into numerical values using Table 2 as follows

$$P_1 = \begin{bmatrix} 1 \\ 5 \end{bmatrix}.$$

Step 5. He converts the above numerical values into binary string 4-bits and therefore P becomes

$$P_2 = \begin{bmatrix} 0001 \\ 0101 \end{bmatrix}.$$

Step 6. Sender further converts the 4-bits binary string into polynomial form and therefore P_1 gives

$$P_3 = \begin{bmatrix} 1 \\ x^2+1 \end{bmatrix}.$$

Step 7. He calculates

$$C = K_1P_3 + S_1^t$$

$$= \begin{bmatrix} x^3+x^2+1 & x+1 \\ x^3+x & x^3+x \end{bmatrix}\begin{bmatrix} 1 \\ x^2+1 \end{bmatrix} + \begin{bmatrix} x \\ x+1 \end{bmatrix}(mod x^4+x+1)$$

$$= \begin{bmatrix} 0 \\ x^3+x^2+1 \end{bmatrix}$$

Using Table 1, we get

$$S_1 = \begin{bmatrix} 0 \\ x^{13} \end{bmatrix}.$$

In order to make the exponent of maximum entries of S_1 as 15 = (2^4-1), we multiply each entry by x^4. Therefore, S_1 becomes

$$S_2 = \begin{bmatrix} 0 \\ x^{17} \end{bmatrix}.$$

and the key matrix

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

is chosen in such a way that if power of x in S_2 is less than 15, the entry in the key matrix is taken 0 otherwise 1.

Step 8. The powers of elements of S_2 are reduced by mod 15 and hence it becomes

$$S_3 = \begin{bmatrix} 0 \\ x^2 \end{bmatrix}.$$

Step 9. The elements of cipher text matrix S_3 are converted into the binary elements as follows

$$S_4 = \begin{bmatrix} 0000 \\ 0100 \end{bmatrix}.$$

The entries of S_4 are converted into numerical values as follows

$$S_5 = \begin{bmatrix} 0 \\ 4 \end{bmatrix}.$$

Further, numerical values are converted into Cipher text $= -C$.

Similar procedure will be followed to convert the remaining plaintext blocks. The converted message is sent through insecure channel.

DECRYPTION:

Step 1. Receiver receives the message. He converts the message into numerical values by using Table 2, which gives

$$S_5 = \begin{bmatrix} 0 \\ 4 \end{bmatrix}.$$

Step 2. He converts the numerical values into binary strings of 3-bits as follows

$$S_4 = \begin{bmatrix} 0000 \\ 0100 \end{bmatrix}.$$

Step 3. Further, he converts binary strings into the elements of $GF(2^4)$, so S_4 becomes

$$S_3 = \begin{bmatrix} 0 \\ x^2 \end{bmatrix}.$$

Step 4. Receiver multiplies only those entries of S_3 by x^{15}, which represents 1 in the matrix K_2.

$$S_2 = \begin{bmatrix} 0 \\ x^{17} \end{bmatrix}.$$

Step 5. He multiplies each entry of S_2 with x^{-4} and obtain

$$S_1 = \begin{bmatrix} 0 \\ x^{13} \end{bmatrix}$$

Further, $S_1(mod x^4 + x + 1)$can be written as

$$S_1 = \begin{bmatrix} 0 \\ x^3 + x^2 + 1 \end{bmatrix}.$$

Step 6. Calculate the key $K_1^{-1} = MS^{-1}M^{-1}$ =

$$\begin{bmatrix} 1 & x^2+1 \\ 1 & x^2+x \end{bmatrix} \begin{bmatrix} x^3 & x^3+1 \\ x^3+x^2+x+1 & x^3+x^2+x \end{bmatrix} \begin{bmatrix} x^2+x & x^2+x+1 \\ x^3+x^2 & x^3+x^2 \end{bmatrix} (mod x^4 + x + 1)$$

$$= \begin{bmatrix} x+1 & x^3+1 \\ x+1 & x^2+1 \end{bmatrix}.$$

Step 7. The receiver calculates

$$P_3 = K_1^{-1}(C_1 - S_1^t)(mod x^4 + x + 1).$$

$$= \begin{bmatrix} x+1 & x^3+1 \\ x+1 & x^2+1 \end{bmatrix} \begin{bmatrix} x \\ x^3+x^2+1+x+1 \end{bmatrix} (mod x^4 + x + 1)$$

$$= \begin{bmatrix} 1 \\ x^2+1 \end{bmatrix}.$$

Step 8. Receiver converts the message into binary strings, which gives

$$P_2 = \begin{bmatrix} 0001 \\ 0101 \end{bmatrix}.$$

Step 9. He converts the binary strings into numerical values as follows

$$P_1 = \begin{bmatrix} 1 \\ 5 \end{bmatrix}.$$

Receiver converts the digits in text by using Table 2 and the plain text $-D$ is obtained. Similar, procedure gives the other blocks of plain text.

CONCLUSIONS: The proposed cipher is the modification of the existing Hill cipher. Use of irreducible polynomial has increased its security. The introduced mechanism in the cipher has created difficulty to the hackers to break the system and retrieve the original message from the cipher text.

REFERENCES

1. 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, 114-118.

2. 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*. 34-37.

3. Hill, L.S. (1929), "Cryptography in an algebraic alphabet" *American Mathematical Monthly*, 36, 306-312.

4. Hill, L. S. (1931), "Concerning certain linear transformation apparatus of cryptography" *American Mathematical Monthly*, 38, 135-154.

5. Ismail, I.A., Amin, M. and Diab, H. (2006), "How to repair Hill cipher*" J. Zhejiang University-Science A*, 7, 2022-2030.

6. Lidl, R. and Niederreiter, H. (1997), "Finite fields, Cambridge University Press, Cambridge, Second Edition".

7. Saeednia's, S. (2000), "How to make the Hill cipher secure" *Cryptologia*, 24, 353-360.

8. Sastry, V.U.K., Murthy, D.S.R. and Bhavani, S.D. (2009), "A block cipher involving a key applied on both sides of the plain text" *International J. Computer and Network Security*, 1, 27-30.

9. Sastry, V. U. K., Murthy, D.S.R. and Bhavani, S. D. (2010), "A block cipher having a key on one side of the plain text matrix and its inverse on the other side" *International Journal of Computer and Network Security*. 2, 1793-8201.

10. Schneier, B. (2007), "Applied cryptography: Protocols, Algorithms and Source Code in C" Second Edition, John Wiley & Sons.

11. Stallings, W. (2006), "Cryptography and network security" Fourth Edition, Pearson.

12. Sharma, P.L. and Kanwar, R.K. (2011), "A note on relationship between invertible rhotrices and associated invertible matrices" *Bulletin of Pure and Applied Sciences*, 30 E (Math & Stat.), 5, 333-339.

13. Sharma, P. L. and Kanwar, R. K. (2012), "Adjoint of a rhotrix and its basic properties" *International J. Mathematical Sciences*, 11, 337-343.

14. Sharma, P. L. and Kanwar, R. K. (2012), "On inner product space and bilinear forms over rhotrices" *Bulletin of Pure and Applied Sciences*, 31E, 109-118.

15. Sharma, P. L. and Kanwar, R. K. (2012), "The Cayley-Hamilton theorem for rhotrices" *International Journal of Mathematics and Analysis*, 4, 171-178.

16. Sharma, P. L. and Kanwar, R. K. (2013), "On involutory and pascal rhotrices" *International J. of Math. Sci. & Engg. Appls. (IJMSEA,*. **7**(IV), 133-146.

17. Sharma, P. L. and Kumar, S. (2013), "On construction of MDS rhotrices from companion rhotrices over finite field" *International Journal of Mathematical Sciences*, 12, 271-286.

18. Sharma, P. L., Kumar, S. and Rehan, M. (2013), "On Hadamard rhotrix over finite field" *Bulletin of Pure and Applied Sciences*, 32 E (Math & Stat.), 181-190.

19. Sharma, P. L., Kumar, S. and Rehan, M. (2013), "On Vandermonde and MDS rhotrices over GF(2^q)" *International Journal of Mathematical and Analysis*, 5, 143-160.

20. Sharma, P.L. and Rehan, M. (2013), "On the security of Hill cipher using finite field" *International Journal of Computer Applications International Journal of Computer Applications*, 71, 30-33.

21. Sharma, P. L. and Rehan, M. (2014), "Modified Hill cipher using Vandermonde matrix and finite field" *International Journal of Technology*. 4, 252- 256.

22. Sharma, P. L. and Sharma, S. (2014), "An application of finite field in Hill cipher" *International Journal of Technology*, 4, 248- 251.

23. Sharma, P. L. and Sharma, S. (2014), "Sequences of irreducible polynomials over GF (2) with three prescribed coefficients" *Recent Trends in Algebra and Mechanics*, 21-32.

24. Sharma, P. L., Sharma, S. and Dhiman, N. (2014), "Construction of infinite sequences of irreducible polynomials using Kloosterman Sum" Bulletin *of Pure and Applied Sciences*, 33, 161-168.

25. Sharma, P. L., Sharma, S. and Rehan, M. (2015), "On construction of irreducible polynomials over F_3" *Journal of Discrete Mathematical Sciences and Cryptography*, 18**,** 335-347.

26. Sharma, P. L., Sharma, S. and Rehan, M. (2015), "Construction of infinite sequences of irreducible polynomials over F_2" *International Journal of Mathematical Sciences & Engineering Applications (IJMSEA*), 9, 19-35.