Encryption and Decryption Technique Involving Finite Fields

Ayush Mittal, Ravindra Gupta

Abstract: ***The object of this paper is to produce a technique for encryption and decryption Involving Finite Fields. In this paper we consider the elements of finite fields GF(2^m) and logical operator XOR to analyze the encryption and decryption technique. Here we also uses the non-singular matrix and a key matrix.***

Key Words: Finite Fields, Logical Operator XOR, Encryption, decryption.

I. INTRODUCTION

The study of secure communications techniques is called Cryptography that permits to view a message and its contents only to the sender and recipient. Cryptography is closely related to encryption.

The original message is known as Plaintext, and Ciphertext is the decrypted message. Plaintext and the Ciphertext both are written in the terms of elements from a finite set A, called an alphabet of description.

Here we establish an algorithm which increases the security of cipher. By making the use of elements of finite fields and logical XOR operator, the proposed algorithm along with illustration involves the encryption and decryption of plaintext.

II. RELATED WORK

Certain encryption and decryption techniques of a message involving group theory, metric space, topological space and finite fields have been established by Rani [6], Okelo [5], Mahdi [4], Arora [1], Kahrobaei [3], Iswariya [2] and others. Looking importance and usefulness of encryption and decryption techniques of a message, we propose to establish a new encryption and decryption techniques of a message involving Finite Fields and Logical Operator XOR, following on the lines of above authors.

III. ALGORITHM

In the proposed algorithm we used two different keys. We choose first key in the form of non-singular matrix and with the help of elements of finite fields, the second key is obtained. During encryption and decryption of the message, the elements of finite fields are used in binary & polynomial form.

3.1 Encryption:

1. Secret key K is shared by Sender and receiver, where K is the $(m-1)\times(m-1)$ non-singular matrix and m is a positive integer.
2. Plaintext is converted by the sender the into pre-assigned numerical values, after then calculates $S = KP(\text{mod}\ (2^m - 1))$. Here *P* is the plain text and S is the first cipher text.
3. Now convert S into binary string of m-bits, we get a matrix M. Again choose a random matrix A of order $(m-1)\times(m-1)$.
4. Randomly select rows/columns of A and perform XOR operation with each row of matrix M and find a matrix M_{XOR}.
5. Converts the entries of M_{XOR} into the elements of $GF(2^m)$. Multiply each entry with α^m and calculate a matrix K' whose entries are 1 if α has the power greater than $2^m - 1$ otherwise 0 and send it to the receiver.
6. Now reduces the powers of the entries to mod $(2^m - 1)$ and find the another matrix $M_{\alpha''}$ (say).
7. Firstly converts each entries of $M_{\alpha''}$ into binary form and then converts such binary entries into the corresponding numerical values. After converting these numerical values into text, finally we get Cipher text.

3.2 Decryption:

1. Receiver finds the message. After converting the message into corresponding numerical values, again converts these numerical values in binary form of m-bits and then change into elements of $GF(2^m)$, we get D_α (say).
2. Now multiplies each entries of D_α with α^{2^m-1} which represents 1 in the corresponding key matrix K' (say) and get a matrix $D_{\alpha'}$ (say).
3. Now multiplies each entries of $D_{\alpha'}$ with α^{-m} and change them in corresponding binary elements of m-bits, we get a matrix $D_{\alpha'''}$ (say).
4. Identifies the rows/columns of matrix A randomly chosen by the sender to perform XOR with each row of the matrix $D_{\alpha'''}$.
5. Now converts each entries of resulting matrix (find in step 4) in numerical values, we get the matrix S.
6. Calculate $P = K^{-1}S(\text{mod}(2^m - 1))$.
7. Now converts each entries of P into corresponding alphabet, we get Plaintext.

IV. ANALYSIS WITH ILLUSTRATION

Consider the numerical values for alphabets and some symbols used in this paper as follows:

Table

alphabet/ symbol	numerical value	alphabet/ symbol	numerical value
@	0	P	16
A	1	Q	17
B	2	R	18
C	3	S	19
D	4	T	20

Revised Manuscript Received on November 30, 2019.

Ayush Mittal, Student, Department of Computer Science Engineering, SRK University, Bhopal, India.

Ravindra Kumar Gupta, Associate Professor, Computer Science Engineering, SRK University, Bhopal, India.

E	5	U	21
F	6	V	22
G	7	W	23
H	8	X	24
I	9	Y	25

J	10	Z	26
K	11	[	27
L	12	\	28
M	13	]	29
N	14	^	30
O	15		

Consider the message [ENCRYPTDECRYPT] as Plaintext.

4.1 Encryption Steps:

1. Let a 4×4 non-singular key matrix K and shares it with the receiver.

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

2. Converts the chosen plain text into corresponding numerical values using above given Table 1, we get,

$$P = \begin{bmatrix} 27 & 5 & 14 & 3 \\ 18 & 25 & 16 & 20 \\ 4 & 5 & 3 & 18 \\ 25 & 16 & 20 & 29 \end{bmatrix}$$

Now calculate S = KP(mod $(2^m - 1)$) on choosing m = 5.

$$\text{KP}(\text{mod } 31) = \begin{bmatrix} 2 & 3 & 5 & 3 \\ 1 & 5 & 1 & 1 \\ 2 & 2 & 3 & 3 \\ 1 & 2 & 1 & 2 \end{bmatrix} \begin{bmatrix} 27 & 5 & 14 & 3 \\ 18 & 25 & 16 & 20 \\ 4 & 5 & 3 & 18 \\ 25 & 16 & 20 & 29 \end{bmatrix} (\text{mod } 31)$$

$$= \begin{bmatrix} 17 & 3 & 27 & 26 \\ 22 & 27 & 24 & 26 \\ 22 & 30 & 5 & 1 \\ 24 & 30 & 27 & 26 \end{bmatrix} = \text{S(say)}$$

3. Converts the numerical values of matrix S into 5-bit binary string, we get

$$M = \begin{bmatrix} 10001 & 00011 & 11011 & 11010 \\ 10110 & 11011 & 11000 & 11010 \\ 10110 & 11110 & 00101 & 00001 \\ 11000 & 11110 & 11011 & 11010 \end{bmatrix}$$

Now randomly consider a 4×4 matrix A as follows:

$$A = \begin{bmatrix} 1 & 1 & 2 & 3 \\ 2 & 3 & 4 & 7 \\ 1 & 2 & 3 & 4 \\ 2 & 2 & 4 & 6 \end{bmatrix}$$

$$= \begin{bmatrix} 00001 & 00001 & 00010 & 00011 \\ 00010 & 00011 & 00100 & 00111 \\ 00001 & 00010 & 00011 & 00100 \\ 00010 & 00010 & 00100 & 00110 \end{bmatrix}$$

4. Choose the rows/columns R_1, R_2, C_2, C_3 from the matrix A at random to perform logical XOR operation with each row of matrix M.

1. Select elements of R_1 of A in 5-bit binary number & performs logical operator XOR with first row of matrix M, we get

   00001000010001000011
   XOR
   10001000111101111010

   which gives the first row of matrix M_{XOR}, as follows

   10000000101100111001

2. Select elements of R_2 of A in 5-bit binary number & performs logical operator XOR with second row of matrix M, we get

   00010000110010000111
   XOR
   10110110111100011010

   which gives the second row of matrix M_{XOR}, as follows

   10100110001110011101

3. Select elements of C_2 of A in 5-bit binary number & performs logical operator XOR with third row of matrix M, we get

   00001000110001000010
   XOR
   10110111100010100001

   which gives the third row of matrix M_{XOR}, as follows

   10111111010011100011

4. Select elements of C_3 of A in 5-bit binary number & performs logical operator XOR with fourth row of matrix M, we get

   00010001000001100100
   XOR
   11000111101101111010

   which gives the fourth row of matrix M_{XOR}, as follows

   11010110101100011110

Hence the matrix M_{XOR} is

$$M_{XOR} = \begin{bmatrix} 10000 & 00010 & 11001 & 11001 \\ 10100 & 11000 & 11100 & 11101 \\ 10111 & 11101 & 00111 & 00011 \\ 11010 & 11010 & 11000 & 11110 \end{bmatrix}$$

5. Now converts the above entries of M_{XOR} into the elements of GF(2^5) in their basis form such that ($\alpha^5 + \alpha^2 + 1$) = 0, we get

$$M_\alpha = \begin{bmatrix} \alpha^4 & \alpha^1 & \alpha^{25} & \alpha^{25} \\ \alpha^7 & \alpha^{21} & \alpha^{21} & \alpha^{14} \\ \alpha^{26} & \alpha^{14} & \alpha^{11} & \alpha^{18} \\ \alpha^9 & \alpha^9 & \alpha^{21} & \alpha^{24} \end{bmatrix}$$

After multiplication by α^5 in the above entries, we get as follows:

$$M_{\alpha'} = \begin{bmatrix} \alpha^9 & \alpha^6 & \alpha^{30} & \alpha^{30} \\ \alpha^{12} & \alpha^{26} & \alpha^{26} & \alpha^{19} \\ \alpha^{31} & \alpha^{19} & \alpha^{16} & \alpha^{23} \\ \alpha^{14} & \alpha^{14} & \alpha^{26} & \alpha^{29} \end{bmatrix}$$

Now choose the key matrix

$$K' = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

such that if power of α in $M_{\alpha'}$ is less than 31, the entry in the key matrix is taken 0 otherwise 1.

6. Now reduce $M_{\alpha'}$ to mod 31, we get

$$M_{\alpha''} = \begin{bmatrix} \alpha^{9} & \alpha^{6} & \alpha^{30} & \alpha^{30} \\ \alpha^{12} & \alpha^{26} & \alpha^{26} & \alpha^{19} \\ \alpha^{0} & \alpha^{19} & \alpha^{16} & \alpha^{23} \\ \alpha^{14} & \alpha^{14} & \alpha^{26} & \alpha^{29} \end{bmatrix}$$

7. Now write the binary form of the elements of cipher text matrix $M_{\alpha''}$, we get

$$S' = \begin{bmatrix} 11010 & 01010 & 10010 & 10010 \\ 01110 & 10111 & 10111 & 00110 \\ 00001 & 00110 & 11011 & 01111 \\ 11101 & 11101 & 10111 & 01001 \end{bmatrix}$$

Again converts the entries of S' into corresponding numerical values, which gives

$$S' = \begin{bmatrix} 26 & 10 & 18 & 18 \\ 14 & 23 & 23 & 6 \\ 1 & 6 & 27 & 15 \\ 29 & 29 & 23 & 9 \end{bmatrix}$$

After converting these numerical values into text using the Table given above, we get the cipher text as follows:

ZJRRNWWFAF[O]]WI

Through public channel, this Cipher text is sent to the receiver.

4.2 Decryption Steps:

1. Take Cipher text message ZJRRNWWFAF[O]]WI. Converts the message into corresponding numerical values using Table as given above, we get

$$S' = \begin{bmatrix} 26 & 10 & 18 & 18 \\ 14 & 23 & 23 & 6 \\ 1 & 6 & 27 & 15 \\ 29 & 29 & 23 & 9 \end{bmatrix}$$

Now converts these numerical values in corresponding binary form of 5-bits, which gives

$$S' = \begin{bmatrix} 11010 & 01010 & 10010 & 10010 \\ 01110 & 10111 & 10111 & 00110 \\ 00001 & 00110 & 11011 & 01111 \\ 11101 & 11101 & 10111 & 01001 \end{bmatrix}$$

Again converts these entries into the elements of $GF(2^5)$ and S' becomes

$$D_{\alpha} = \begin{bmatrix} \alpha^{9} & \alpha^{6} & \alpha^{30} & \alpha^{30} \\ \alpha^{12} & \alpha^{26} & \alpha^{26} & \alpha^{19} \\ \alpha^{0} & \alpha^{19} & \alpha^{16} & \alpha^{23} \\ \alpha^{14} & \alpha^{14} & \alpha^{26} & \alpha^{29} \end{bmatrix}$$

2. Multiplies those entries of D_{α} with α^{31} which represents 1 in the corresponding key matrix K', we get the following transformed matrix:

$$D_{\alpha'} = \begin{bmatrix} \alpha^{9} & \alpha^{6} & \alpha^{30} & \alpha^{30} \\ \alpha^{12} & \alpha^{26} & \alpha^{26} & \alpha^{19} \\ \alpha^{31} & \alpha^{19} & \alpha^{16} & \alpha^{23} \\ \alpha^{14} & \alpha^{14} & \alpha^{26} & \alpha^{29} \end{bmatrix}$$

3. Now multiply $D_{\alpha'}$ with α^{-5}, we get

$$D_{\alpha''} = \begin{bmatrix} \alpha^{4} & \alpha^{1} & \alpha^{25} & \alpha^{25} \\ \alpha^{7} & \alpha^{21} & \alpha^{21} & \alpha^{14} \\ \alpha^{26} & \alpha^{14} & \alpha^{11} & \alpha^{18} \\ \alpha^{9} & \alpha^{9} & \alpha^{21} & \alpha^{24} \end{bmatrix}$$

So the binary representation of $D_{\alpha''}$ is

$$D_{\alpha'''} = \begin{bmatrix} 10000 & 00010 & 11001 & 11001 \\ 10100 & 11000 & 11100 & 11101 \\ 10111 & 11101 & 00111 & 00011 \\ 11010 & 11010 & 11000 & 11110 \end{bmatrix}$$

4. Now recognizes the rows/columns R_1, R_2, C_2, C_3 into 5-bit binary number of the matrix A, which is chosen by the sender, as follows:

$$A = \begin{bmatrix} 1 & 1 & 2 & 3 \\ 2 & 3 & 4 & 7 \\ 1 & 2 & 3 & 4 \\ 2 & 2 & 4 & 6 \end{bmatrix} = \begin{bmatrix} 00001 & 00001 & 00010 & 00011 \\ 00010 & 00011 & 00100 & 00111 \\ 00001 & 00010 & 00011 & 00100 \\ 00010 & 00010 & 00100 & 00110 \end{bmatrix}$$

1. Select elements of R_1 of A in 5-bit binary number & performs logical operator XOR with first row of matrix $D_{\alpha'''}$, we get

   00001000010001000011
   XOR
   10000000101100111001

   which gives the first row of matrix M, as follows

   10001000111101111010
2. Select elements of R_2 of A in 5-bit binary number & performs logical operator XOR with second row of matrix $D_{\alpha'''}$, we get

   00010000110010000111
   XOR
   10100110001110011101

   which gives the second row of matrix M, as follows:

   10110110111100011010
3. Select elements of C_2 of A in 5-bit binary number & performs logical operator XOR with third row of matrix $D_{\alpha'''}$, we get

   00001000110001000010
   XOR
   10111111010011100011

   which gives the third row of matrix M, as follows

   10110111100010100001
4. Select elements of C_3 of A in 5-bit binary number & performs logical operator XOR with fourth row of matrix $D_{\alpha'''}$, we get

   00010001000001100100
   XOR
   11010110101100011110

   which gives the fourth row of matrix M, as follows

   11000111101101111010

   Therefore the matrix M is

$$M = \begin{bmatrix} 10001 & 00011 & 11011 & 11010 \\ 10110 & 11011 & 11000 & 11010 \\ 10110 & 11110 & 00101 & 00001 \\ 11000 & 11110 & 11011 & 11010 \end{bmatrix}$$

5. Now converts the entries of M into corresponding numerical values, we get

$$S = \begin{bmatrix} 17 & 3 & 27 & 26 \\ 22 & 27 & 24 & 26 \\ 22 & 30 & 5 & 1 \\ 24 & 30 & 27 & 26 \end{bmatrix}$$

6. Calculate $P = K^{-1}S(\text{mod } 31)$. Therefore,

$$P = K^{-1}S(\text{mod } 31)$$

$$= \begin{bmatrix} 27 & 26 & 11 & 23 \\ 17 & 3 & 11 & 3 \\ 23 & 14 & 25 & 14 \\ 20 & 8 & 2 & 10 \end{bmatrix} \begin{bmatrix} 17 & 3 & 27 & 26 \\ 22 & 27 & 24 & 26 \\ 22 & 30 & 5 & 1 \\ 24 & 30 & 27 & 26 \end{bmatrix} (\text{mod } 31)$$

$$= \begin{bmatrix} 27 & 5 & 14 & 3 \\ 18 & 25 & 16 & 20 \\ 4 & 5 & 3 & 18 \\ 25 & 16 & 20 & 29 \end{bmatrix}$$

7. Now converts the digits of the above matrix into corresponding alphabet using the given Table, we get plain text as follows:

[ENCRYPTDECRYPT]

V. RESULT AND DISCUSSION

On the cipher, the cryptanalysis is done. Here key length is 4×4 matrix in this cipher. Therefore, due to this reason Brute force attack cannot be able to break the cipher.

Also known plain text attack cannot break the Cipher text because plain text and the cipher text having no relation directly even if key matrix is known in detail. Since key is depending on logical XOR operation and it displaces the binary bits at different phases of iteration, therefore resultant cipher having highly strength.

VI. CONCLUSION

Proposed encryption and decryption technique is based on the elements of finite fields. It produces two levels of security. In this technique, for different block data, the second key is different, which gives difficulty for breaking the cryptosystem. Thus, there are minimum prospects for Brute force attack. Since here no direct relation between plain text and cipher text, therefore the cipher text cannot be broken (even if the key matrices are known) with the known plain text attack.

REFERENCES

1. Arora Priya, Use of Group Theory in Cryptography, IJARIIE-ISSN(O)-2395-4396, Vol-2, Issue-6, 2016, pp. 1767-1772.
2. Iswariya S., Rishivarman A. R.: An Arithmetic Technique for Non-Abelian Group Cryptosystem, International Journal of Computer Applications (0975 – 8887), Volume 161, No 2, March 2017, pp. 32-35.
3. Kahrobaei Delaram, Anshel Michael: Applications of Group Theory in Cryptography, International Journal of Pure and Applied Mathematics, Volume 58, No. 1, 2010, pp. 21-23.
4. Mahdi Hamza Abedal-Hamza, Al-khafaji Saba Nazar Faisel: Using the Connected Components of Topological Spaces in Cryptography, International Journal of Mathematics Trends and Technology, Volume 12, Number 1, Aug 2014, pp. 31-33.
5. Okelo N. B.: Properties of Complete Metric Spaces and their Applications to Computer Security, Information and Communication Technology: Evolving Trends in Engineering and Technology Online: 2014-08-04, ISSN: 2349-915X, Vol. 1, pp 23-28.
6. Rani Asha, Jyoti Kumari: A New Approach to Public Key Transferring Algorithm Scheme Using Metric Space, IOSR Journal of Mathematics (IOSR-JM) e-ISSN: 2278-5728, p-ISSN: 2319-765X, Volume 12, Issue 1 Ver. III (Jan. - Feb. 2016), pp. 04-06.

AUTHORS PROFILE

Mr.Ayush Mittal did his post-graduation in M.Tech(Master of Technology) in Computer Science and Engineering from Indian Institute of Information Technology and Management(IIITM),Gwalior, MP in 2015. He has also received gold medal in post-graduation degree. Currently, he is pursuing his Phd in Computer Science and Engineering from SRK university, Bhopal, MP. His area of interest includes robotics, cryptography and embedded systems. He has published 2 research papers in International Journals.

Dr. Ravindra kumar Gupta received his M.Tech (Master of Technology) degree in Computer Science & Engineering from Sri Satya Sai Institute Of Science & Technology, RGPV Bhopal, In 2010 M.P., Ph.D in Computer Science & Enginnering From Barkatullah University Bhopal India. Presently he is Associate Professor Of Computer Science and Engineering Department in RKDFIST,BHOPAL,M.P. India. He is having 12 Yrs of teaching experience .He has published 54 papers in referred International/National Journal & conference also a Member of Easy Chair Conference System.