A Cryptographic Scheme of Finite Fields using Logical Operators

G.Naga Lakshmi
Assistant Professor
Department of Mathematics
GITAM University

B.Ravi Kumar
Assistant Professor
Department of Mathematics
GITAM University

Ch.Suneetha
Assistant Professor
Department of Mathematics
GITAM University

A.Chandra Sekhar
Professor
Department of Mathematics
GITAM University

ABSTRACT

Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the massage. With widespread availability of computer technology, the rapid growth of wireless communications secured exchange of information has become a challenging task. The most basic of the modules in modern cryptography is that of a primitive, which may be regarded as a cryptographic building block which performs one or more desired functions, and may be combined with others to form a cryptographic protocol. The most well-known and perhaps the simplest primitive is encryption, which allows parties to achieve confidential data transmission over an insecure channel. In the present paper we proposed a cryptographic technique using elements of a finite field and logical operators basing on inverse property. To test the efficacy of the proposed scheme the cryptanalysis is performed.

Keywords:

Encryption, Decryption, Logical XNOR Operator, Finite Fields, key matrix.

1. INTRODUCTION

In cryptography frequently used mathematical operations are addition, subtraction and multiplication.

1.1 Finite Fields:

Let F be a non-empty set. Then F is called a Field if F is an abelian group under addition and multiplication. If the number of elements in F is finite then the field is finite. The positive integers are stored in the computer as n-bit words where n is usually 8, 16, 32, 64, and soon. Therefore the range of integers is 0 to 2^n - 1. The Galois field GF (p) with set Z_p where p is the largest prime number less than 2^n where as GF (2^n) is a finite field having 2^n elements. The elements in this field are n-bit words, [4] [5].

1.2 Logical Operators:

An XNOR gate is a digital logic gate that performs a logical operation on one or more logic inputs and produces a single logic output. Several researchers used the application of logical XNOR Operation in Cryptography [1]. The sequence of numbers generated by a Linear Feed Back Shift Register or its XNOR counterpart is used especially in military cryptography [3]. In the present paper we use logical XNOR Operations and the field GF(2^n) for encryption/decryption of the messages.

Example:

The GF (2^3) has 8 elements are {0, 1, g, g^2,g^3,g^4,g^5,g^6} using the irreducible polynomial of f(x) = x^3+x+1, which means that g^3+g+1 = 0 or g^3 = g + 1. Other powers of g can be calculated accordingly. The following shows the valued of the g's.

0	000	$g^3 = g + 1$	011
1	001	$g^4 = g^2 + g$	110
g	010	$g^5 = g^2 + g + 1$	111
g^2	100	$g^6 = g^2 + 1$	101

2. PROPOSED WORK

Let $A = \begin{bmatrix} 2 & 5 & 2 & 6 \\ 7 & 6 & 2 & 5 \\ 3 & 3 & 3 & 5 \\ 3 & 3 & 3 & 6 \end{bmatrix}$ be a randomly taken 4x4 matrix.

2.1 Encryption

Suppose sender wants to send the message "GOOD".

Step1: sender converts these plane text characters into 4 – bit string using ASCII code and writes these numbers in form of 4x4 matrixes M, [2].

The message matrix

$$M = \begin{bmatrix} 0111 & 1111 & 1111 & 0100 \\ 0000 & 0000 & 0000 & 0000 \\ 0000 & 0000 & 0000 & 0000 \\ 0000 & 0000 & 0000 & 0000 \end{bmatrix}.$$

Step 2: Sender selects the rows/ columns C_2 R_3 C_4 C_1 form the matrix A at random to perform the logical XNOR Operation with each row of matrix A. Sender converts the elements of C_2 into 4-bit binary numbers, [6] [7][8].

0101011000110011

Step 3: Sender performs logical XNOR operation between the binary stream of first row of message matrix M and the binary stream that sender obtained at step2.

0111111111110100

XNOR

0101011000110011

result is 1st row of M_{XNOR} 1101011000111000

Step 4: Similarly sender converts the elements of R_3, C_4, C_1 of the matrix A into 4-bit binary numbers and performs logical XNOR operation between the binary streams of 2nd, 3rd and 4th row of message matrix M.

0000000000000000

XNOR

0011001100110101

result is 2nd row of M_{XNOR} 1100110011001010

and 0000000000000000

XNOR

0110010101010110

result is 3rd row of M_{XNOR} 1001101010101001

And 0000000000000000

XNOR

0010011100110011

result is 4th row of M_{XNOR} 1101100011001100

This results in M_{XNOR}.

$$M_{XNOR} = \begin{bmatrix} 1101 & 0110 & 0011 & 1000 \\ 1100 & 1100 & 1100 & 1010 \\ 1001 & 1010 & 1010 & 1001 \\ 1101 & 1000 & 1100 & 1100 \end{bmatrix}.$$

Step 5: sender converts the above entries to the elements of GF (2^4).

$$M_2 = \begin{bmatrix} g^{13} & g^5 & g^4 & g^3 \\ g^6 & g^6 & g^6 & g^9 \\ g^{14} & g^9 & g^9 & g^{14} \\ g^{13} & g^3 & g^6 & g^6 \end{bmatrix}$$

Step 6: Sender multiply M_2 by g^4 then

$$M_3 = \begin{bmatrix} g^{17} & g^9 & g^8 & g^7 \\ g^{10} & g^{10} & g^{10} & g^{13} \\ g^{18} & g^{13} & g^{13} & g^{18} \\ g^{17} & g^7 & g^{10} & g^{10} \end{bmatrix}.$$

Step 7: M_3 is reduced to mod 15 resulting in

$$M_4 = \begin{bmatrix} g^2 & g^9 & g^8 & g^7 \\ g^{10} & g^{10} & g^{10} & g^{13} \\ g^3 & g^{13} & g^{13} & g^3 \\ g^2 & g^7 & g^{10} & g^{10} \end{bmatrix}$$ and the key matrix

$$K=\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$ is chosen in such a way that the first entry in the key matrix is 1 because $17 \equiv 2 \mod 1x15$ and if powers of g in M_3 is less than 15 the entry in the key matrix is taken as 0.

Step 8: The cipher text

$$M_4 = \begin{bmatrix} g^2 & g^9 & g^8 & g^7 \\ g^{10} & g^{10} & g^{10} & g^{13} \\ g^3 & g^{13} & g^{13} & g^3 \\ g^2 & g^7 & g^{10} & g^{10} \end{bmatrix}$$

Step 9: These elements convert to the binary elements

$$C = \begin{bmatrix} 0100 & 1010 & 0101 & 1011 \\ 0111 & 0111 & 0111 & 1101 \\ 1000 & 1101 & 1101 & 1000 \\ 0100 & 1011 & 0111 & 0111 \end{bmatrix}$$

Then all the binary elements of the matrix C are coded to the text characters using ASCII code which be called the first Cipher text DJEKGGGMHMMHDKGG.

This cipher text is sent to receiver in the public channel.

2.2 Decryption:

The receiver receive the message

“DJEKGGGMHMMHDKGG”.

Step1: converts the received message characters into 4 – bit string using ASCII code and writes these 16 binary numbers in the form of a 4x4 matrix.

$$C = \begin{bmatrix} 0100 & 1010 & 0101 & 1011 \\ 0111 & 0111 & 0111 & 1101 \\ 1000 & 1101 & 1101 & 1000 \\ 0100 & 1011 & 0111 & 0111 \end{bmatrix}$$

Step 2: Receiver converts the above 4-bit binary number into the elements of GF (2^4).

$$D_1 = \begin{bmatrix} g^{2} & g^{9} & g^{8} & g^{7} \\ g^{10} & g^{10} & g^{10} & g^{13} \\ g^{3} & g^{13} & g^{13} & g^{3} \\ g^{2} & g^{7} & g^{10} & g^{10} \end{bmatrix}$$

Step 3: By multiplying the key with 15 and on adding the D_1 we get

$$D_2 = K+D_1 = \begin{bmatrix} g^{17} & g^{9} & g^{8} & g^{7} \\ g^{10} & g^{10} & g^{10} & g^{13} \\ g^{18} & g^{13} & g^{13} & g^{18} \\ g^{17} & g^{7} & g^{10} & g^{10} \end{bmatrix}$$

Step 4: Receiver multiply D_2 by g^{-4} then

$$D_3 = g^{-4} \text{ x } D_2 = \begin{bmatrix} g^{13} & g^{5} & g^{4} & g^{3} \\ g^{6} & g^{6} & g^{6} & g^{9} \\ g^{14} & g^{9} & g^{9} & g^{14} \\ g^{13} & g^{3} & g^{6} & g^{6} \end{bmatrix}$$

Step 5: Receivers convert the above elements into the 4-bit binary elements

$$\text{Then } D_4 = \begin{bmatrix} 1101 & 0110 & 0011 & 1000 \\ 1100 & 1100 & 1100 & 1010 \\ 1001 & 1010 & 1010 & 1001 \\ 1101 & 1000 & 1100 & 1100 \end{bmatrix}$$

Step 6: Receiver recognizes the rows/columns C_2 R_3 C_4 C_1 the matrix A selected by sender to perform the logical XNOR operation with the rows of the matrix M_{XNOR} form the algorithm in a separate communication. Receiver converts the elements C_2 into 4-bit binary format as

0101011000110011

Step 7: The logical XNOR operation is performed between the binary steam of first row of matrix D_4 and binary steam that is obtained in step 6.

1101011000111000

XNOR

0101011000110011

result in 1st row of M

0111111111110100

Step 8: similarly the logical XNOR operation is performed between the binary steams of 2nd 3rd 4th row of matrix D_4 and binary steams of R_3 ,C_4 ,C_1 into 4-bit binary. That means

1100110011001010

XNOR

0011001100110101

result is 2nd row of M

0000000000000000

And

1001101010101001

XNOR

0110010101010110

result is 3rd row of M

0000000000000000

And 1101100011001100

XNOR

0010011100110011

result is 4th row of M

0000000000000000

This results in M.

$$M = \begin{bmatrix} 0111 & 1111 & 1111 & 0100 \\ 0000 & 0000 & 0000 & 0000 \\ 0000 & 0000 & 0000 & 0000 \\ 0000 & 0000 & 0000 & 0000 \end{bmatrix}.$$

Step 9: All the elements of the matrix M which are in 4-bit binary format are converted to the text characters using ASCII code table to get the original message "GOOD".

3. CRYPTANALYSIS

The cryptanalysis on the cipher is done. In this cipher the length of the key is 4X4 matrix . Due to this fact the cipher cannot be broken by Brute force attack.

The Cipher cannot be broken with known plain text attack as there is no direct relation between the plain text and the cipher text even if the details of the key matrix are known.It is noted that the key dependent logical XNOR operation plays an important role in displacing the binary bits at various stages of iteration, and this induces enormous strength to the cipher.

4. CONCLUSIONS:

In the proposed work secret key is using elements of finite field to increase the security level and logical XNOR operation. It is difficult to decipher the encrypted message as the key is private between the communicating parties and the key is different for different data block is generated from the secret key agreed upon by the communicating parties .The cryptanalysis shows the strength of the proposed scheme.

5. REFERENCES

[1] A.P. Stakhov, "The golden matrices and a new kind of Cryptography", Chaos, Solution and Fractals 32(2007) pp1138-1146.

[2] Bon Wook Hwan Seok Jang Hwan Song, "On Constructing a 32x32 binary matrices as a Di ussinsg Layer for a 256-Bit Block Cipher, Lecture Notes in Computer Science, 2006 Vol.4296/2006,51-64.

[3] Chen-Hun-Chen, YenJui-Cheng and Guo Juin-In, "Design a New Cryptography system", Lecture Notes in Computer Science 2002, Vol. 2532/2002, 211-219.

[4] Hun-Chen Chen, Jui Cheng Yen, "A new Cryptography systems and its VISI Realization", Journal of Systems Architecture, Vol.49, Issues 7-9, October 2003, pages 355-367.

[5] Martine Hell and Thomas Johnson, "Breaking the Stream Cipher F-FCSR- H and F-FCSR-16 in Real Time", Journal of Cryptology, October 2009.

[6] Wang Pengjun Lu Jingang Jian Xu and Jing Dai, "Power Optimization algorithm based on XNOR/OR logic", Journal of Electronics Vol. 26, 2009-Issue (1), 138-144.

[7] Xevgenity Dodis and John Steinberg, "Message Authentication Codes from Unpredictable Block Ciphers", Lecture Notes in Computer Science, Vol.5677/2009.

[8] D.Sravana Kumar, Ch.Suneetha and A.Chandra Sekhar " A Block Cipher Using Logical XNOR and NOT Operations". International Journal of Science and Advanced Technology (ISSN 2221-8386) Volume 1 No 4 June2011.