IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 11, Issue 2 Ver. II (Mar - Apr. 2015), PP 01-04
www.iosrjournals.org

A Method of Designing Block Cipher Which Involves a Key Bunch Matrix with Polynomial Entries over F_2

SAJU M I[1], LILLY P L[2]

1Assistant Professor, Department of Mathematics, St. Thomas' College, Thrissur, Kerala, India.
2Associate professor, Department of Mathematics, St. Joseph's College, Irinjalakuda, India.

Abstract: *In this paper , we have devoted our attention to the development of block cipher , which involves a key bunch matrix , an additional matrix , and key matrix utilized in the development of a pair of functions called permute and substitute , over a finite extension field of F_2 . The entries of the matrices are polynomials over $F_{2,}$ this create confusion and diffusion for each round of the iteration process of the encryption algorithm. The security of this process depends upon the size of the extension field. This cipher cannot be broken by any cryptanalytic attack generally available in the literature of cryptography.*

***Key words**: Function field, Key bunch matrix, Permute, Primitive polynomial, Substitute.*

I. Introduction

Block cipher is a type of symmetric cipher in which Plaintext is divided into blocks of fixed length and every block is encrypted one at a time. A block cipher is a set of 'code books' and every key produce a different code book. The encryption of a plaintext block is the corresponding cipher text block entry in the code book.

Security of information, which has to be maintained in a secret manner, is the primary concern of all the block ciphers. We have studied several block ciphers [1] [2] [3]. In the present paper, our objective is to modify the block cipher, presented in [4], by including the matrices with polynomial entries over F_2. Here our interest is to see how the shift, the affine and the additional key matrix would act in strengthening the cipher.

II. Development Of The Cipher

Consider a function field $\frac{F_2[x]}{(f(x))}$, where f(x) is a primitive polynomial of degree n over F_2. Let α be a root of f(x). Then α^r be a polynomial of α [5][6].
Consider a plaintext matrix P, given by,
$P = [\alpha^{p_{ij}}]$,$i = 1$ to $k, j = 1$ to k. (2.1)
Let us take the key bunch matrix E in the form
$E =[\alpha^{e_{ij}}]$, $i = 1$ to $k, j = 1$ to k. (2.2)
Here we take all e_{ij} as odd numbers, which lie in the interval $[1, 2^n - 1]$. On using the concept of multiplicative inverse, we get the decryption key bunch matrix D, in the form
$D = [\alpha^{d_{ij}}]$, $i = 1$ to $k, j = 1$ to k. (2.3)
Where e_{ij} and d_{ij} are related by the relation $e_{ij}\ d_{ij} \equiv 1 (\mathrm{mod} 2^n - 1)$ for all i and j. (2.4)
Here, it is to be noted that d_{ij} will be obtained as odd numbers and lie in the interval $[1, 2^n - 1]$
The additional key matrix F, can be taken in the form
$F = [\alpha^{f_{ij}}]$, $i = 1$ to k, $j = 1$ to k. (2.5)
Where f_{ij} are integers lying in$[1, 2^n - 1]$ .The basic equations governing the encryption and the decryption in this analysis are given by,
$C = [\alpha^{c_{ij}}]$, where $c_{ij} \equiv ((e_{ij} p_{ij})(\mathrm{mod} 2^n - 1) + f_{ij})(\mathrm{mod} 2^n - 1)$, $i = 1$ to $k, j = 1$ to k. (2.6)
And $P = [\alpha^{p_{ij}}]$, where $p_{ij} \equiv (d_{ij}(c_{ij} - f_{ij}))(\mathrm{mod} 2^n - 1)$, $i = 1$ to k, $j = 1$ to k. (2.7)
Where C is the cipher text. We use shift cipher and affine cipher as permute and substitute round functions.

III. Illustration Of The Cipher

Consider a function field $\frac{F_2[x]}{(f(x))}$, where $f(x) = x^5 + x^3 + 1$ is the primitive polynomial of degree 5 over F_2. Let α be a root of $f(x)$. Then α^r be a polynomial of α..

r	α^r	r	α^r
1	α	2	α^2
3	α^3	4	α^4
5	$\alpha^3 + 1$	6	$\alpha^4 + \alpha$
7	$\alpha^3 + \alpha^2 + 1$	8	$\alpha^4 + \alpha^3 + \alpha$
9	$\alpha^4 + \alpha^3 + \alpha^2 + 1$	10	$\alpha^4 + \alpha + 1$

11	$\alpha^3+\alpha^2+\alpha+1$	12	$\alpha^4+\alpha^3+\alpha^2+\alpha$
13	$\alpha^4+\alpha^2+1$	14	$\alpha+1$
15	$\alpha^2+\alpha$	16	$\alpha^3+\alpha^2$
17	$\alpha^4+\alpha^3$	18	$\alpha^4+\alpha^3+1$
19	$\alpha^4+\alpha^3+\alpha+1$	20	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$
21	$\alpha^4+\alpha^2+\alpha+1$	22	$\alpha^2+\alpha+1$
23	$\alpha^3+\alpha^2+\alpha$	24	$\alpha^4+\alpha^3+\alpha^2$
25	α^4+1	26	$\alpha^3+\alpha+1$
27	$\alpha^4+\alpha^2+\alpha$	28	α^2+1
29	$\alpha^3+\alpha$	30	$\alpha^4+\alpha^2$
31	1		

α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	α^{15}	α^{16}
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
α^{17}	α^{18}	α^{19}	α^{20}	α^{21}	α^{22}	α^{23}	α^{24}	α^{25}	α^{26}	α^{27}	α^{28}	α^{29}	α^{30}	α^{31}	
Q	R	S	T	U	V	W	X	Y	Z		.	?	,	!	

Consider the plaintext **MATHS DEPARTMENT**

$$P = \begin{bmatrix} \alpha^{13} & \alpha^1 & \alpha^{20} & \alpha^8 \\ \alpha^{19} & \alpha^{27} & \alpha^4 & \alpha^5 \\ \alpha^{16} & \alpha^1 & \alpha^{18} & \alpha^{20} \\ \alpha^{13} & \alpha^5 & \alpha^{14} & \alpha^{20} \end{bmatrix}$$

Encryption:

Take a key bunch matrix $E = \begin{bmatrix} \alpha^1 & \alpha^3 & \alpha^5 & \alpha^7 \\ \alpha^3 & \alpha^3 & \alpha^3 & \alpha^3 \\ \alpha^1 & \alpha^1 & \alpha^1 & \alpha^1 \\ \alpha^5 & \alpha^7 & \alpha^5 & \alpha^7 \end{bmatrix}$

Take additional key matrix $F = \begin{bmatrix} \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 \\ \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 \\ \alpha^2 & \alpha^1 & \alpha^3 & \alpha^1 \end{bmatrix}$

Then $\left[\alpha^{(e_{ij}\,p_{ij})(\text{mod } 31)}\right] = \begin{bmatrix} \alpha^{13} & \alpha^3 & \alpha^7 & \alpha^{25} \\ \alpha^{26} & \alpha^{19} & \alpha^{12} & \alpha^{15} \\ \alpha^{16} & \alpha^1 & \alpha^{18} & \alpha^{20} \\ \alpha^3 & \alpha^4 & \alpha^8 & \alpha^{16} \end{bmatrix}$ and

$\left[\alpha^{(e_{ij}\,p_{ij})(\text{mod } 31)+f_{ij}\,)(\text{mod } 31)}\right] = \begin{bmatrix} \alpha^{14} & \alpha^5 & \alpha^{10} & \alpha^{29} \\ \alpha^{29} & \alpha^{23} & \alpha^{17} & \alpha^{21} \\ \alpha^{22} & \alpha^8 & \alpha^{26} & \alpha^{29} \\ \alpha^5 & \alpha^5 & \alpha^{11} & \alpha^{17} \end{bmatrix}$

Apply shift cipher with key **‘4’**

$$= \begin{bmatrix} \alpha^{18} & \alpha^9 & \alpha^{14} & \alpha^2 \\ \alpha^2 & \alpha^{27} & \alpha^{21} & \alpha^{25} \\ \alpha^{26} & \alpha^{12} & \alpha^{30} & \alpha^2 \\ \alpha^9 & \alpha^9 & \alpha^{15} & \alpha^{21} \end{bmatrix}$$

Apply affine cipher with key **(3, 2)**

$$C = \begin{bmatrix} \alpha^{25} & \alpha^{29} & \alpha^{13} & \alpha^8 \\ \alpha^8 & \alpha^{21} & \alpha^3 & \alpha^{15} \\ \alpha^{18} & \alpha^7 & \alpha^{30} & \alpha^8 \\ \alpha^{29} & \alpha^{29} & \alpha^{16} & \alpha^3 \end{bmatrix}$$

So the cipher text will be **Y?MHHUCORG,H?PC**

Decryption:

$$C = \begin{bmatrix} \alpha^{25} & \alpha^{29} & \alpha^{13} & \alpha^8 \\ \alpha^8 & \alpha^{21} & \alpha^3 & \alpha^{15} \\ \alpha^{18} & \alpha^7 & \alpha^{30} & \alpha^8 \\ \alpha^{29} & \alpha^{29} & \alpha^{16} & \alpha^3 \end{bmatrix}$$

Apply affine cipher with key **(21, 20)**

$$= \begin{bmatrix} \alpha^{18} & \alpha^9 & \alpha^{14} & \alpha^2 \\ \alpha^2 & \alpha^{27} & \alpha^{21} & \alpha^{25} \\ \alpha^{26} & \alpha^{12} & \alpha^{30} & \alpha^2 \\ \alpha^9 & \alpha^9 & \alpha^{15} & \alpha^{21} \end{bmatrix}$$

Apply shift cipher with key **‘27’**

$$\mathbf{S} = \begin{bmatrix} \alpha^{14} & \alpha^{5} & \alpha^{10} & \alpha^{29} \\ \alpha^{29} & \alpha^{23} & \alpha^{17} & \alpha^{21} \\ \alpha^{22} & \alpha^{8} & \alpha^{26} & \alpha^{29} \\ \alpha^{5} & \alpha^{5} & \alpha^{11} & \alpha^{17} \end{bmatrix}$$

$$\left[\alpha^{(s_{ij}-f_{ij})(\bmod 31)}\right] = \begin{bmatrix} \alpha^{13} & \alpha^{3} & \alpha^{7} & \alpha^{25} \\ \alpha^{26} & \alpha^{19} & \alpha^{12} & \alpha^{15} \\ \alpha^{16} & \alpha^{1} & \alpha^{18} & \alpha^{20} \\ \alpha^{3} & \alpha^{4} & \alpha^{8} & \alpha^{16} \end{bmatrix}$$

The decryption key bunch matrix D = $[d_{ij}]$, where $d_{ij}e_{ij} \equiv 1(\mathrm{mod}31)$.

Then D = $\begin{bmatrix} \alpha^{1} & \alpha^{21} & \alpha^{25} & \alpha^{9} \\ \alpha^{21} & \alpha^{21} & \alpha^{21} & \alpha^{21} \\ \alpha^{1} & \alpha^{1} & \alpha^{1} & \alpha^{1} \\ \alpha^{25} & \alpha^{9} & \alpha^{25} & \alpha^{9} \end{bmatrix}$ and

$$P = \left[\alpha^{\left(d_{ij}(s_{ij}-f_{ij})\right)(\bmod 31)}\right] = \begin{bmatrix} \alpha^{13} & \alpha^{1} & \alpha^{20} & \alpha^{8} \\ \alpha^{19} & \alpha^{27} & \alpha^{4} & \alpha^{5} \\ \alpha^{16} & \alpha^{1} & \alpha^{18} & \alpha^{20} \\ \alpha^{13} & \alpha^{5} & \alpha^{14} & \alpha^{20} \end{bmatrix}$$

So the plain text will be **MATHS DEPARTMENT**

ALGORITHM FOR ENCRYPTION:

```
1.  Read P,E, F,n,r
2.  For k = 1 to r do
    {
3.  For i = 1 to n do
    {
4.  For j = 1 to n do
             {
5.  $p_{ij}$ = ($e_{ij}$*$p_{ij}$) mod31
    }
6.  $p_{ij}$ = ([$p_{ij}$] +$f_{ij}$) mod 31
        }
7.  $p_{ij}$ = ([$s_{ij}$+t]) mod 31
      }
8.  $p_{ij}$ = (u$a_{ij}$+v) mod 31
      }
9.  C = P
10. Write (C)
    ALGORITHM FOR DECRYPTION:
1.  Read C,E, F,n,r
2.  D = Mult (E)
3.  For k = 1 to r do
    {
4.  For i = 1 to n do
    {
5.  For j = 1 to n do
    {
6.  $c_{ij}$= [$u^{-1}c_{ij}$+-$u^{-1}$v] (mod 31)
                  }
7.  $c_{ij}$ = [$a_{ij}$-t] (mod 31)
     }
8.  $c_{ij}$ = [ $d_{ij}$*($s_{ij}$-$f_{ij}$) ] mod31
                 }
9.  C = [$c_{ij}$]
    }
10. P = C
11. Write (P)
```

IV. Cryptanalysis

In the development of all the block ciphers, the importance of cryptanalysis is commendable. The different cryptanalytic attacks that are dealt with very often in the literature of cryptography are

1. Cipher text only attack.
2. Known plaintext attack.
3. Chosen plaintext attack.
4. Chosen cipher text attack.

Let us consider the cipher text only attack. In this analysis, we have three important entities namely, the key bunch matrix E, the additional key matrix F and the special key K, used in the Shift and Affine functions. On account of these three, the number of possible keys is a large number. Another important remark in the above block cipher, the entries of the matrices is polynomials. So this cannot be broken by the cipher text only attack.

Now let us examine the known plain text attack. In the case of this attack, we know any number of plaintext and cipher text pairs, which we require for our investigation. Focusing our attention on r =1, that is on the first round of the iteration process , in the encryption , we get the set of equations, given by

$$P = \left(\left([e_{ij}\,p_{ij}]\text{mod } 31\right) + F\right)\text{mod}31, i = 1 \text{ to } n, j = 1 \text{ to } n, \quad (4.1)$$

$$P = \text{Shift}(P) \quad (4.2)$$

$$P = \text{Affine}(P) \quad (4.3)$$

and

$$C=P \quad (4.4)$$

Here as C in (4.4) is known, we get P. However, as the shift process and affine process depend upon the key, one cannot have any idea regarding shift and affine. Thus it is impossible to determine P even at the next higher level that is in (4.3). In a spectacular manner, if one has a chance to know the key used in the shift and affine, then one can determine P, occurring on the left hand side of (4.1). Then it is not at all possible to determine the e_{ij}. At the same time the entries are polynomials over F_2, so we conclude that this cipher cannot be broken by the known plain text attack.

V. Conclusions

In this paper, we have developed a block cipher which involves an encryption key bunch matrix, an additional matrix and a key matrix utilized for the development of a pair of functions called shift and affine. This cipher is more strengthen when the entries of the matrices are polynomials of F_2. The cryptanalysis carried out in the investigation firmly indicates that this cipher cannot be broken by any cryptanalytic attack. The programmers required for encryption and decryption are written in Java. Here it may be noted that this cipher can be applied for the encryption of a plain text of any size. In this cipher the role of algebraic function field is very important.

References

[1]. Dr.V.U.K. Sastry, K.Shirisha, A Novel Block Cipher Involving a Key Bunch Matrix, International Journal of Computer Applications, 55(16), 2012, 1-6(6)

[2]. Dr. V.U.K. Sastry, K.Shirisha, A Block Cipher Involving a Key Bunch Matrix and Including another Key Matrix supplemented with Xor Operation, International Journal of Computer Applications, 55(16), 2012, 7-10(4)

[3]. Dr. V.U.K. Sastry, K.Shirisha, A Block Cipher Involving a Key Bunch Matrix and Including Another Key Matrix supported with Modular Arithmetic Addition, International Journal of Computer Applications 55(16), 2012, 11-14(4)

[4]. Dr. V.U.K. Sastry, K.Shirisha, A Block Cipher Involving a Key Bunch Matrix and an Additional Key Matrix, Supplemented with Modular Arithmetic Addition and Supported by Key-Based Substitution, International Journal of Advanced Computer Science and Applications (IJACSA), 3(12), 2012, 110-115(6)

[5]. Dr. Lilly P.L., Saju M.I., A Method of Designing a Public-Key Cryptosystem Based on Discrete Logarithm Problem, International Journal of Pure Algebra, 4(11), 2014, 628-630(3)

[6]. Saju M.I., Dr. Lilly P.L., A Public-Key Cryptosystem Based on Discrete Logarithm Problem over Finite Fields F_{p^n}, IOSR Journal of Mathematics, 11(1), 2015, 01-03(3)