© 2016 IJSRST | Volume 2 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher

Robbi Rahim*[1], Ali Ikhwan[2]

[1]Faculty of Computer Science, Universitas Pembangunan Panca Budi, Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing, 20122, Medan, Sumatera Utara, Indonesia
[2]Faculty of Science and Technology, Universitas Islam Negeri Sumatera Utara, Jl. Willem Iskandar Pasar V Medan Estate, 20371, Medan, Sumatera Utara, Indonesia

ABSTRACT

There are many data security techniques like a cryptography, there are many algorithm like a MMB (Modular Multiplication Block Cipher) and Playfair Cipher. MMB operates using 128-bit plaintext, but it also uses 32-bit subblock MMB text (x0, x1, x2, x3) and 32-bit key subblock (k0, k1, k2, k3) and then the fundamental of this algorithm is determined by a multiplication modulo operation 2^{32}-1. Different from MMB, playfair cipher is a diagram substitution cipher which takes two letter from message and replace with two another pair letter, this paper combines playfair cipher as a key substitution and messages in plaintext to be encrypted with algorithms MMB, this combination is expected to increase the security level of messages.

Keyword: Cryptography, Encryption, Combination Algorithm, MMB, Playfair Cipher

I. INTRODUCTION

Cryptography is an ubiquitous tool in the world of information security [1] [2] [3]. It is required when trying to keep the secrecy of communications over open channels or to prove the authenticity of an incoming message, it can be used to create many multiparty protocols in a way that makes cheating difficult and expensive [1]. In fact, its range of applicability is very wide and it would not be possible to give a complete list of functionalities that can be achieved through the use of cryptography. Instead, we are going to focus on a small set of fundamental goals and see how they can be formalized into precise security notions. From an historical perspective, the oldest and foremost cryptographic goal is confidentiality [1], when talking about cryptography there are many method than can be used, few of them is MMB and Playfair cipher, MMB which is a kind of modern cryptographic algorithms and Playfair cipher which is a kind of classical algorithms, in this paper both methods will be combined to produce a better ciphertext [4] [5].

Cryptography MMB method using 128-bit plaintext and iterative algorithm consisting of linear steps (such as XOR and key applications) as well as the parallel application of the four major non-linear substitution which can be reversed [3] [5]. This substitution is determined by a multiplication modulo operation 2^{32}-1 with a constant factor, which has a higher level of security when compared with the method that uses only IDEA multiplication modulo 2^{16} + 1 MMB using 32 bit subblock text (x0, x1, x2, x3) and 32-bit key subblock (k0, k1, k2, k3). This makes the algorithm very suitable implemented on 32-bit processors. A non-linear function, f, applied six times along with XOR [3] [6].

Different from modern algorithms such as MMB which uses mathematical calculations [3], Playfair cipher algorithm it uses the substitution of the alphabet that are 25 letters like caesar ciphers or cipher vigenere. Playfair Cipher encrypt pairs of letters (digraphs), instead of single letters as is the case with simpler substitution ciphers such as the Caesar Cipher. Frequency analysis is still possible on the Playfair cipher, however it would be against 600 possible pairs of letters instead of 26 different possible letters. For this reason the Playfair cipher is much more secure than older substitution ciphers [4].

The playfair cipher starts with creating a key table. The key table is a 5×5 grid of letters that will act as the key

for encrypting your plaintext. Each of the 25 letters must be unique and one letter of the alphabet (usually Z) is omitted from the table (as there are 25 spots and 26 letters in the alphabet) [4].

Based explanation in paragraph above, in this paper how to combine two different cryptographic algorithms to produce a better ciphertext, the joint combination algorithm applied to the encryption key and plaintext to be encrypted using MMB algorithm, the first step taken is the key and the plaintext encrypted beforehand using Playfair algorithm and the result of the encryption algorithm Playfair to be encrypted again using MMB algorithm so that the message will be safer than before, because MMB algorithm converts the readable data into the non-readable data. although it is possible that the ciphertext can be penetrated by using techniques such as brute force.

II. METHODS AND MATERIAL

A. Theory

Weakness IDEA method that uses a 64-bit plaintext and multiplication modulo 2^{16} + 1, corrected by Joan Daemen in an algorithm called MMB (Modular Multiplication-based Block cipher) [1] [5]. By using plaintext 64 bit (4 pieces of 16-bit subblock text), IDEA method can only be implemented on 16-bit processors, thus judged not to follow the progress of technology at this point that most have used the 32-bit processors. Cryptography MMB method using 128-bit plaintext and iterative algorithm consisting of linear steps (such as XOR and key applications) as well as the parallel application of the four major non-linear substitution which can be reversed [5]. This substitution is determined by a multiplication modulo operation 2^{32}-1 with a constant factor, which has a higher level of security when compared with the method that uses only IDEA multiplication modulo 2^{16} + 1 MMB using 32 bit subblock text (x0, x1, x2, x3) and 32-bit key subblock (k0, k1, k2, k3). This makes the algorithm very suitable implemented on 32-bit processors. A non-linear function, f, applied six times along with XOR function [5].

First step is to generate the key, use the MMB method along the 128-bit key. The process of forming the key to the method is very simple MMB. The key-input is only divided into 4 pieces subblock key lengths of 32 bits each [3] [5]. The process of formation is the key to the MMB method can be seen in the following chart:

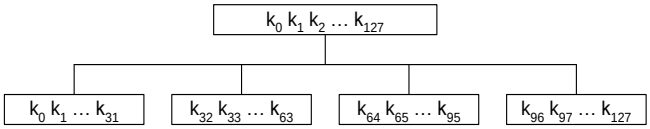

Figure 1. MMB Key Formation Process

MMB method using the plaintext and the key length of 128 bits [5]. The core of the encryption process of MMB method is as follows:

1. The plaintext is divided into 4 equal subblock (x0, x1, x2, x3) .
2. Perform the following process 2 times: (Index performed modulo operation 4)

```
for i = 0 to 3
      xi = xi XOR ki
next i
f (x0, x1, x2, x3)
for i = 0 to 3
      xi = xi XOR ki + 1
next i
f (x0, x1, x2, x3)
for i = 0 to 3
      xi = xi XOR ki + 2
next i
f (x0, x1, x2, x3)
```

Diagram of the process is looking like the following picture

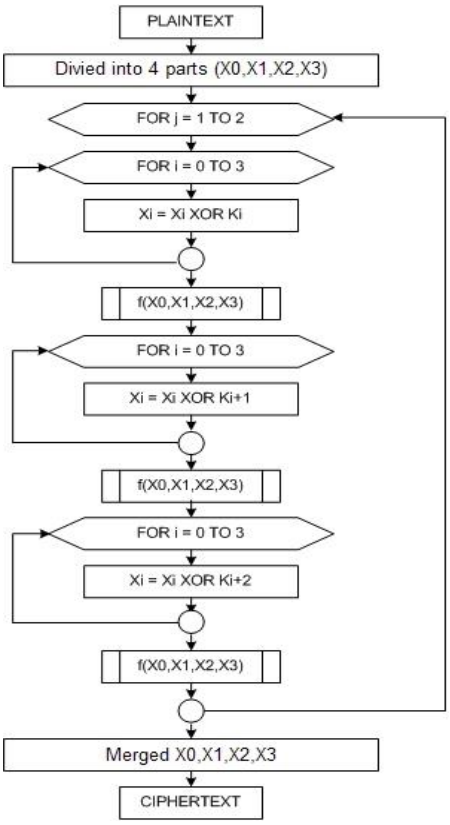

Figure 2. Encryption process on MMB Methods

After the encryption process, the next is the decryption process that is used to return the results of the ciphertext into plaintext.

The algorithm used in the decryption process is slightly different than the encryption process. The essence of the method MMB decryption process can be described as follows:

1. Ciphertext is divided into 4 equal subblock (x0, x1, x2, x3) [5].
2. Perform the following process 2 times: (Index performed modulo operation 4)

```
f (x0, x1, x2, x3)
for i = 0 to 3
    xi = xi XOR ki + 2
next i
f (x0, x1, x2, x3)
for i = 0 to 3
    xi = xi XOR ki + 1
next i
f (x0, x1, x2, x3)
for i = 0 to 3
    xi = xi XOR ki
next i
```

Diagram of the decryption process is looking like the following picture

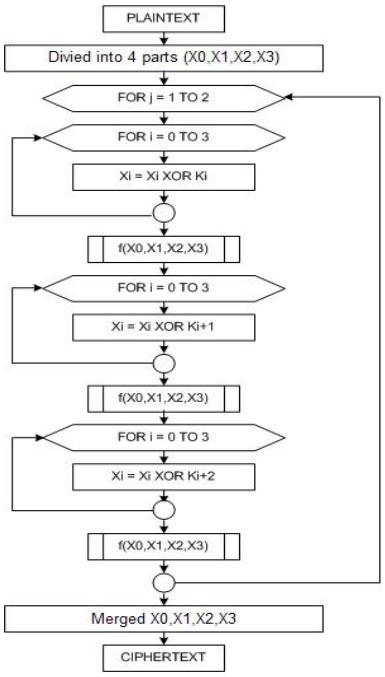

Figure 3. Decryption process on MMB Methods

Playfair cipher used by the British Army during the Second Boer War and World War I. First discovered by Sir Charles Wheatstone and Baron Lyon Playfair on March 26, 1854. Playfair are digraphs cipher, meaning that every encryption process performed on each of two letters. Suppose plaintext "cryptology", then it becomes "cryptology" [7]. Playfair using a 5x5 table. All of the alphabet except J is placed into the table. J considered the same as the letter I, because the frequency of occurrence of the letter J has the smallest. The key that is used in the form of words and no repeating the same letter. If the key "MATAHARI", then the key used is "MATHRI". Furthermore, the key is inserted into a 5x5 table, the first field is the key, then write the letters in sequence subsequent advance of the first line, if the letter had appeared, it was not written back

Here are the rules of the encryption process at Playfair:

1. If the second letter is not in line and the same column, then the first letter be a line of letters with letters column first and second letters. The second letter is capitalized in same row with both the letter and the same column with the first letter.
2. If the second letter is located on the line the same first letter to uppercase later in the same line, so also with the second letter. If located in fifth row, then

became the first row, and vice versa. Its direction depends on the the first and second positions, the shift in the direction of the second letter.

3. If the second letter is located on the column the same first letter to uppercase later in the same column, as well as the second letter. If located on the fifth column, it becomes The first column, and vice versa. Its direction depending on the position of the first letter and second, the shift in the direction of the second letter.
4. If the two letters together, then place a letter in the middle (in accordance agreement).
5. If the number of letters of plaintext is odd, then add one letter in the end, as the rules of the 4th.

While the decryption process is the inverse of the encryption process.

B. Proposed Method

The first step is to determine the plaintext (T), which will first be encrypted using Playfair cipher algorithm to produce ciphertext (T_1), the results of Playfair cipher encryption (T_1) to be encrypted again with MMB algorithm to produce ciphertext (T) and also for decryption, below is a diagram of how the encryption and decryption.

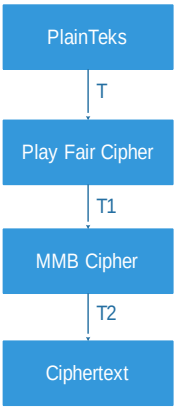

Figure 4. Flowchart Representating Encrypt Playfair and MMB

Decryption process is not much different from the encryption process, the process is done by first decrypting the new MMB algorithm followed by Playfair cipher, the following diagram is shown below

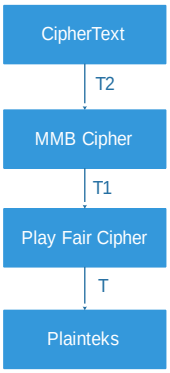

Figure 5. Flowchart Representating Decrypt Playfair and MMB

As an example of the application process and the Playfair cipher MMB algorithm can be described as follows:

plaintext "UNIVERSITYPAHANG" with key "NARUTO", the key and the plaintext is processed by the Playfair cipher and the results are as follows:

Table 1. Key of Cipher

N	A	R	U	T
O	B	C	D	E
F	G	H	I	K
L	M	P	Q	S
V	W	X	Y	Z

Having obtained the results above, the following is expanding key arrangement in the square by adding the sixth column and the sixth row, the key table will be:

Table 2. Key Expansion

N	A	R	U	T	N
O	B	C	D	E	O
F	G	H	I	K	F
L	M	P	Q	S	L
V	W	X	Y	Z	V
N	A	R	U	T	

Encryption is done depends on the type of couple letters against a reference table. In general The letter pair is divided into three types: both are in the same line, both in the field the same, or both are not in rows and columns the same one.

a. If the letter pairs are in the same line, then they will be substituted with the letter the first on the right of

each letter. If one of the letters contained in the right end of it will be replaced with the letter the far right of the row

b. If there is a letter pair in column same, then they will be substituted with The first letter in the bottom of each letter. If one letter located at the lower end it will be replaced with the letter of the top of the column

c. If a letter is not in column and the same row, then use different approach. To replace The first letter, browse the rows of letters The first to arrive in the column containing the second letter, the letter contained at the intersection of columns and rows will replace the first letter. Do the same for the second letter.

After the above process is done, the results obtained ciphertext of town " UNIVERSITYPAHANG " is " TA FY CT QK UZ MR GR AF ".

After getting ciphertext from Playfair encryption algorithm, encryption result then encrypted again using MMB algorithm, here is the process of using the encryption key "UNIVERSITYPAHANG" and plaintext "TAFYCTQKUZMRGRAF ", the first step to do is to convert the existing key into binary so that key "UNIVERSITYPAHANG" will be shown below
Key = “UNIVERSITYPAHANG”, and the binary result is

01010101010011100100100101010110010001010101001000101001101001001010101000101100101010000010000010100100001000001010011100100011

divided into four (4) pieces of the key sub-blocks into

K(0) = 01010101010011100100100101010110
K(1) = 01000101010100100101001101001001
K(2) = 01010100010110010101000001000001
K(3) = 01001000010000010100111001000111

After the formation of the key successfully, the next is doing the encryption process based on the key and the plaintext, the results are as follows:
Plaintext = TAFYCTQKUZMRGRAF
Conversion to binary:

01010100010000010100011001011001010100010000010100011001011001
10001010001010010111010101010110100100110101
01001001000111010100100100000101000110

The results of the conversion of plaintext binary converted into 4 pieces of text subblock, 4 (four) sub-blocks as shown below

X(0) = 01010100010000010100011001011001
X(1) = 01000011010101000101000101001011
X(2) = 01010101010110100100110101010010
X(3) = 01000111010100100100000101000110

After knowing the binary of each key and plaintext, using XOR function value of each existing sub key and plaintext are calculated, as shown below

X(0) = X(0) XOR K(0)
= 01010100010000010100011001011001 XOR
01010101010011100100100101010110
= 00000001000011110000111100001111

X(1) = X(1) XOR K(1)
= 01000011010101000101000101001011 XOR
01000101010100100101001101001001
= 00000110000001100000001000000010

X(2) = X(2) XOR K(2)
= 01010101010110100100110101010010 XOR
01010100010110010101000001000001
= 00000001000000110001110100010011

X(3) = X(3) XOR K(3)
= 01000111010100100100000101000110 XOR
01001000010000010100111001000111
= 00001111000100110000111100000001

X(0) = C(0) * X(0) MOD ((2^32) - 1)
= 00000010010111110001110011011011 *
00000001000011110000111100001111 MOD
11111111111111111111111111111111
= 01000010000110110000100010101000

X(1) = C(1) * X(1) MOD ((2^32) - 1)
=00000000000000000000000010010111110001110011
10110110 * 00000110000001100000001000000010
MOD 11111111111111111111111111111111
= 00100100010100000111000101000101

X(2) = C(2) * X(2) MOD ((2^32) - 1)
=00000000000000000000000100101111100011100110
11011000 * 00000001000000110001110100010011
MOD 11111111111111111111111111111111
= 00100111001110101100111000000001

X(3) = C(3) * X(3) MOD ((2^32) - 1)
=00000000000000000001001011111000111001101101
10000000 * 00001111000100110000111100000001
MOD 11111111111111111111111111111111
= 00111010010110001101111101000111

If LSB(X(0)) =
LSB(01000010000110110000100010101000) = 0 = 1 --
> FALSE

If LSB(X(3)) =
LSB(00111010010110001101111101000111) = 1 = 0 --
> FALSE

Iteration process continues until the known value of the LSB X (0) = 1, the final results of the iteration process as below

If LSB(X(0)) =
LSB(10101001001000000001101111111001) = 1 = 1 --
> TRUE

X(0) = X(0) XOR C
= 10101001001000000001101111111001 XOR
00101010101010101010101010101010
= 10000011100010101011000101010011

If LSB(X(3)) =
LSB(11111010001100010100000001110110) = 0 = 0 --
> TRUE

X(3) = X(3) XOR C
= 11111010001100010100000001110110 XOR
00101010101010101010101010101010
= 11010000100110111110101011011100

X(0) = X(3) XOR X(0) XOR X(1)
= 11010000100110111110101011011100 XOR
10000011100010101011000101010011 XOR
11111001011111111000010010110000
= 10101010011011101101111100111111

X(1) = X(0) XOR X(1) XOR X(2)
= 10101010011011101101111100111111 XOR
11111001011111111000010010110000 XOR
10011111011101000011011011110001
= 11001100011001010110110101111110

X(2) = X(1) XOR X(2) XOR X(3)
= 11001100011001010110110101111110 XOR
10011111011101000011011011110001 XOR
11010000100110111110101011011100
= 10000011100010101011000101010011

X(3) = X(2) XOR X(3) XOR X(0)
= 10000011100010101011000101010011 XOR
11010000100110111110101011011100 XOR
10101010011011101101111100111111
= 11111001011111111000010010110000

Result:10101010011011101101111100111111110110
00110010101101101011111101000001110001010101 1
00010101001111111001011111111000010010110000

Ciphertext =
20c2aa6ec39f3fc38c656d7ec692c5a0c2b153c3 b97f
e2809ec2b0

After getting the ciphertext of the encryption process, the next step is to decrypt, decryption steps performed in accordance with the measures contained in Figure 5, The following result are shown below

CipherText
=20c2aa6ec39f3fc38c656d7ec692c5a0c2b153c3 b97f
e2809ec2b0

Conversion to binary:

10101010011011101101111100111111110110001100
10101101101011111101000001110001010101100010 1
01001111111001011111111000010010110000
X(0) = 10101010011011101101111100111111
X(1) = 11001100011001010110110101111110
X(2) = 10000011100010101011000101010011
X(3) = 11111001011111111000010010110000

Decryption process is carried out from the sub-blocks the largest to the smallest, as shown below.
X(3) = X(2) XOR X(3) XOR X(0)

= 10000011100010101011000101010011 XOR
11111001011111111000010010110000 XOR
10101010011011101101111100111111
= 11010000100110111110101011011100
X(2) = X(1) XOR X(2) XOR X(3)
= 11001100011001010110110101111110 XOR
10000011100010101011000101010011 XOR
11010000100110111110101011011100
= 10011111011101000011011011110001
X(1) = X(0) XOR X(1) XOR X(2)
= 10101010011011101101111100111111 XOR
11001100011001010110110101111110 XOR
10011111011101000011011011110001
= 11111001011111111000010010110000
X(0) = X(3) XOR X(0) XOR X(1)
= 11010000100110111110101011011100 XOR
10101010011011101101111100111111 XOR
11111001011111111000010010110000
= 10000011100010101011000101010011

Almost the same as encryption, decryption process will be done if the LSB (X0) and LSB (X) = 0, then the result as below

If LSB(X(0)) =
LSB(01000010000110110000100010101000) = 0 = 1 --> FALSE
If LSB(X(3)) =
LSB(00111010010110001101111101000111) = 1 = 0 --> FALSE
X(0) = C(0) * X(0) MOD ((2^32) - 1)=
00001101101011010100011010010100 *
01000010000110110000100010101000 MOD
11111111111111111111111111111111
= 00000001000011110000111100001111
X(1) = C(1) * X(1) MOD ((2^32) - 1)=
00000110110101101010001101001010000000000000000000000000000000 *
00100100010100000111000101000101 MOD
11111111111111111111111111111111
= 00000110000001100000001000000010
X(2) = C(2) * X(2) MOD ((2^32) - 1) =
00011011010110101000110100101000000000000000000000000000000000 *
00100111001110101100111000000001 MOD
11111111111111111111111111111111
= 00000001000000110001110100010011
X(3) = C(3) * X(3) MOD ((2^32) - 1)=
00011011010110101000110100101000000000000000000000000000000000 * 00111010010110001101111101000111 MOD 11111111111111111111111111111111
= 00001111000100110000111100000001
X(0) = X(0) XOR K(0)
= 00000001000011110000111100001111 XOR
01010101010011100100100101010110
= 01010100010000010100011001011001
X(1) = X(1) XOR K(1)
= 00000110000001100000001000000010 XOR
01000101010100100101001101001001
= 01000011010101000101000101001011
X(2) = X(2) XOR K(2)
= 00000001000000110001110100010011 XOR
01010100010110010101000001000001
= 01010101010110100100110101010010
X(3) = X(3) XOR K(3)
= 00001111000100110000111100000001 XOR
01001000010000010100111001000111
= 01000111010100100100000101000110
Result=01010100010000010100011001011001010000110101010001010001010010110101010101011010010011101010100100100011101010010010000010100011

Ciphertext For Playfair= TAFYCTQKUZMRGRAF

After the plaintext obtained using MMB decryption algorithm, then the next step are decrypting using Playfair algorithm, the following result are shown below

Table 3. Key Expansion For Decrypt

N	**A**	R	U	**T**	N
O	B	C	D	E	O
F	G	H	I	K	F
L	M	P	Q	S	L
V	W	X	Y	Z	V
N	A	R	U	T	

It appears that the characters on the same line position but not side by side, for it was taken the position that the characters on the left, while the other letters to the couple in accordance with the rules of the Playfair cipher, the plaintext from the ciphertext results are "UNIVERSITYPAHANG". decryption process is successfully done by combining two different algorithms and the result is maximal.

III. MERITS AND DEMERITS

Merits

It has been proposed a cryptosystem by combining two cryptographic algorithms MMB & Playfair Cipher.

Demerits

The disadvantage is in the encryption and decryption process because involving two different algorithms requires additional time to process

IV. CONCLUSION

The security of the data may be improved by combining the two ciphers of MMB and Playfair, because the complexity of two algorithm the result of ciphertext also much more complicated than using one algorithm.

V. REFERENCES

[1] A. Joux, Algorithmic Crypanalysis, United States: CRC Press, 2009.

[2] J. Seberry, Cryptography: An Introduction to Computer Security (Advances in Computer Science Series), Prentice Hall, 1989.

[3] K. Jia, J. Chen, M. Wang and X. Wang, "Practical-time Attack on the Full MMB Block Cipher," International Association for Cryptologic Research, 2010.

[4] A. Alam, S. Khalid and M. Salam, "A Modified Version of Playfair Cipher Using 7," IJCTE, pp. 626-628, 2013.

[5] M. Wang, J. Nakahara and Y. Sun, "Cryptanalysis of the full MMB block ciphe," InfoScience, pp. 234-251, 2003.

[6] S. V.U.K and K. Shirisha, "A Block Cipher Involving a Key Matrix and a Key bunch Matrix, Supplemented with Mix," International Journal Of Engineering And Science, vol. II, no. 9, pp. 37-43, 2013.

[7] A. Negi, J. S. Farswan, V. Thakkar and S. Ghansala, "Cryptography Playfair Cipher using Linear Feedback Shift Register," IOSR Journal of Engineering, vol. II, no. 5, pp. 1212-1216, 2012.