RESEARCH ARTICLE OPEN ACCESS

Modification Application of Key Metrics 13x13 Cryptographic Algorithm Playfair Cipher and Combination with Linear Feedback Shift Register (LFSR) on Data Security Based on Mobile Android

[1]Denni Kurniawan, [2]April Lia Hananto, [3]Bayu Priyatna
[1](Univesity Budi Luhur, Jakarta, Indonesia)
[2,3](University Buana Perjuangan, Karawang, Indonesia)

----------**********----------

Abstract:

Playfair cipher is a classic encryption method that is difficult to manually manipulate but apart from the advantages found in plyafair cipher there are also many shortcomings, can be solved by using the information frequency of occurrence bigram, can not enter lowercase letters, numbers and special characters when encrypting This research modifies the key matrix of playfair cryptography algorithms and combines with the Linear Feedback Shift Register (LFSR) algorithm, by changing the size of the 13x13 key matrix the playfair cipher is able to insert characters as many as 196 characters consisting of capital letters, lowercase letters. The result of calculation with avalanche effect method got average value 43,59% at playfair cipher done by modification of matrix key 13x13 and combined with LFSR generator, 2,15% at playfair cipher 10x10 matrix key without merged with LFSR and 34,41% at playfair classic 5x5. That the playfair cipher that has been modified and combined with the LFSR generator is stronger than the previous playfair cipher. The result of time complexity testing has fast encryption and decryption.

Keywords **— Playfair, LFSR, cryptography, encryption, description.**

----------**********----------

I. INTRODUCTION

Data will be important if it produces useful information for a person or an institution or company, in general, important information will always generate high value validation in accordance with the principle of the information itself that is reliable and authenticity of the source. It does not rule out that very important and high value information can be targeted by criminals, who deliberately want to exploit the weaknesses of both conventional and modern systems such as theft and data destruction. The techniques that can be used to maintain the contents of a data is very diverse one of them is by using cryptography techniques (Chryphtography). Cryptography itself comes from the Greek word "cryptós" which means secret, while "gráphein" means writing, so if combined into "secret writing". Currently cryptography is often used in many ways, especially to maintain information security such as confidentiality/privacy, data integrity, authentication and nonrepudiation used for authentication (Simbolon, 2016).

Examples of cryptographic techniques used both classical and modern, such as, Vigenere, Playfair, AES, RSA and many others. According to Bhat [1], the results of a comparison analysis between AES, RSA and Playfair Cipher cryptography, that Playfair Cipher excels in securing data efficiently and unambiguously. According to Mahyudin [2], Playfair Cipher should be used to disguise important messages needed quickly.

Then [3], Playfair Cipher is a classic encryption method that is difficult to manually analyze. An important component of the playfair algorithm is the

cipher table used for encrypting and decrypting the default table introduced by playfair is a table that has a matrix of size (5x5) containing the capital letters of AZ by omitting the letter J. Although the text security on the Playfair cipher algorithm this is very difficult to analyze, but it can still be solved by using the information frequency of occurrence bigram.

In addition to these problems [4], the classic Playfair cipher algorithm still has a number of weaknesses such as not being able to enter lowercase letters, numbers and special characters while encrypting. The resultant ciphertext of the playfair algorithm is easily solved when a cryptanalysis knows the ciphertext and its cipher table, although cryptanalis only knows its ciphertext without knowing that the cryptanalyst chiper table can guess the bigram by meaningful letters from a word [5]. Although by modifying the contents of the squares key by simply shifting according to the number of columns, then actually the key is repeated every 5 times. Thus this will result in a gap for conducting cryptanalysis [6].

Judging from these factors, the authors are interested in modifying the key matrix of the Playfair cryptography algorithm and combining it with other cryptographic algorithms, then implementing the modified Playfair cryptography algorithm into an application program and applied to secure data.

II. THEORETICAL BASIS

A. *Cryptography / Cryptography*

Cryptography (cryptography) in Greek is divided into two terms namely "cryptós" which has a secret meaning, while "gráphein" means writing, from both terms combined to become "secret writing" [7]. The beginning of cryptography is the science and art to maintain the confidentiality of the message by encoding into a form that can not be understood anymore meaning. Then along with the development of cryptography is no longer limited to encrypt the message, but also provides aspects of security against attacks from cryptanalysis. Therefore, the notion of cryptografipun turned into science as well as art to maintain the security of messages [8].

B. *Playfair Cipher Cryptography*

Playfair Cipher is a symmetric symmetric substitution key substitution. Techniques used in conventional playfair ciphers split plaintext in sets of two characters each known as digraphs. Namely is composed of the alphabet as identification. The playfair password algorithm is formed using the 5 × 5 matrix of 25 letters created as shown in Figure II-1. The key matrix required for the encryption and description process is built by placing letters of the keyword without repetition from left to right and from top to bottom in the matrix, and then the remaining matrix completes with the remaining alphabets in alphabetical order. And change the letter "J" to "I" if it is on plaintext [9].

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

Figure II-1 Sample Key Matrix [9].

C. *Playfair Cipher Encryption Algorithm*

Before performing the encryption process, the plaintext to be encrypted is set first as follows :

1. All characters and spaces that do not belong to the alphabet must be removed first from plaintext (if any).
2. If there is a letter J on the plaintext do the changes with the letter I.
3. Plaintext into the original message done arrangement according to the letter pair (bigram).
4. When there is a pair of the same letter then do change one letter of the letter pair with the letter Z or X insert it by using the letter X because the letter X is very minimal in the same bigram, unlike the letter Z, for example is the word FUZZY.
5. If the letters on the plaintext have an odd number then select an additional letter then add at the end of the plaintext. Additional letters can be selected for example the letter Z or X.

D. *Algorithm Description Plafair Cipher*

Here is the stage of the playfair cipher algorithm:

1. If there are two letters located on the same key row then each letter is changed using the letters on the left.
2. If there are two letters located on the same column then each letter is changed with the letter above it.
3. If two letters are not on the same row and column, change them to the letter in the first line intersection with the two letter columns. Then next the second letter is changed using letters at the fourth vertex of the rectangle formed from the letters used [3].

E. ***Linear Feedback Shift Register (LFSR)***

LFSR is a register that shifts with a certain amount, output is selected and added modulo 2. Also fed back to the input register at each clock cycle. LFSR itself consists of N storage elements called stages. An N-stage LFSR is characterized by an N × N matrix, called TSR. The format and size of the TSR is based on the feedback stage dependence. Furthermore, the state is a linear function of the previous state [10].

III. SYSTEM DESIGN

The research methodology used in this research is engineering, Theoretical Computer Science where the researcher uses a cryptographic technique with modification method of playfair algorithm table using 13x13 matrix and combining it with Linear Feedback Shift Register (LFSR) 8 bits. The process flow of systematic process from this research is poured in figure III-1 as follows:

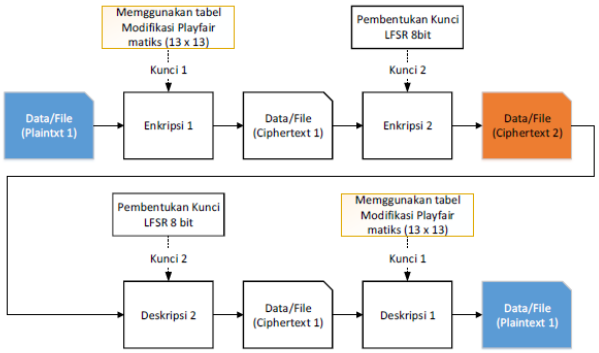


Figure III-1 Flow of Data Security System

A. ***Playfair 13x13 Matic***

The establishment of a 13 x 13 playfair matrix table of keys entered, in the formation of keys consisting of letters, numbers and symbols Suppose the key example "IM @ Ululu5". The first step is a key consisting of numbers, letters or symbols should not have more than one appearance if there is such thing then remove the numbers, letters or symbols that have in common. So the key of "AkuM @ Ululu5" becomes "AkuM @ Ul5". In Table III-2 is a matrix formed from the key "AkuM @ U15":

A	k	u	M	@	U	1	5	B	C	D	E	F
G	H	I/J	K	L	N	O	P	Q	R	S	T	V
W	X	Y	Z	a	b	c	d	e	f	g	h	i/j
m	n	o	p	q	r	s	t	v	w	x	y	z
0	1	2	3	4	6	7	8	9	®	©	╬	¶
Đ	┤	_	^	&	*	(	)	-	=	+	[	@
]	;	„	:	“	\	,	.	/	<	>	?	~
£	¥	|	ß	π	σ	µ	#	∞	±	≥	≤	{
÷	{	}	Ă	Ā	Ė	É	Ē	Ĕ	Ī	Ĭ	Ĩ	}
Ĭ	Đ	Ń	Ó	Ó	Ó	Õ	Ō	Ø	Ú	Ú	Ú	!
Ý	Á	á	â	ä	Å	Ω	Ç	è	É	ê	ë	⌈
ì	Í	î	ï	ð	Ñ	ò	Ó	ô	Õ	ù	⌂	$
₊	˥	∑	≠	ğ	€	Ω	λ	Ľ	Đ	Ī	Ý	⊣

Figure r III-2 Playfair 13x13 Matriks

B. ***Linear Feedback Shift Register (LFSR)***

The step in the data encryption method using linear feedback Shift Register (LFSR) 8 bits, is the formation of the key matrix. Here is an illustration of the key formation process of LFSR key :

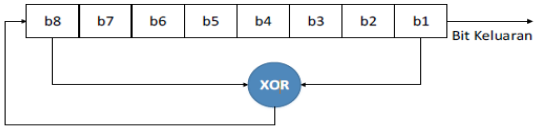
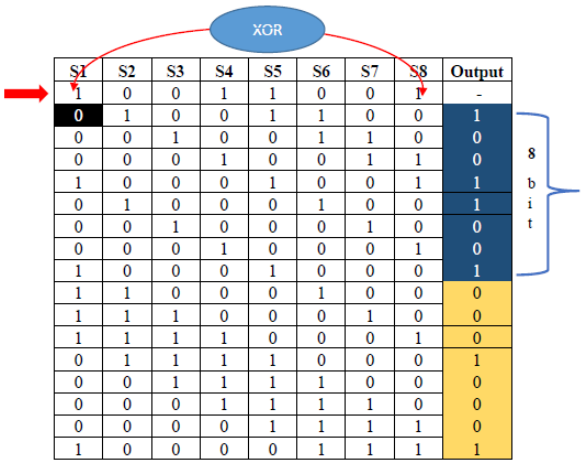


Figure III-3 Key Formation Process

In the illustration above illustrates the stage or process flow in key formation with 8 bit LFSR. Where b1, b2, ... b8 represent an input bit b1 xor b8 then b8 is shifted and placed in the output bit. Here are the results of the LFSR key building process :



S1	S2	S3	S4	S5	S6	S7	S8	Output
1	0	0	1	1	0	0	1	-
0	1	0	0	1	1	0	0	1
0	0	1	0	0	1	1	0	0
0	0	0	1	0	0	1	1	0
1	0	0	0	1	0	0	1	1
0	1	0	0	0	1	0	0	1
0	0	1	0	0	0	1	0	0
0	0	0	1	0	0	0	1	0
1	0	0	0	1	0	0	0	1
1	1	0	0	0	1	0	0	0
1	1	1	0	0	0	1	0	0
1	1	1	1	0	0	0	1	0
0	1	1	1	1	0	0	0	1
0	0	1	1	1	1	0	0	0
0	0	0	1	1	1	1	0	0
0	0	0	0	1	1	1	1	0
1	0	0	0	0	1	1	1	1

Figure III-4 Establishment of LFSR Keys

In the above table enter initial input 10011001 then the resulting output is 10011001 then the next output is 00010001 and so on until (n). Then the resulting output compiles into a matrix of size (2 × n) where length (n) is based on the length of the row contained in ciphertexts which has been generated from the 1st encryption process, using playfair cipher.

IV. RESULT AND DISCUSSION

A. ***Construction User Interface***

The built application user interface can be seen in Figure IV-1 and Figure IV-2 :

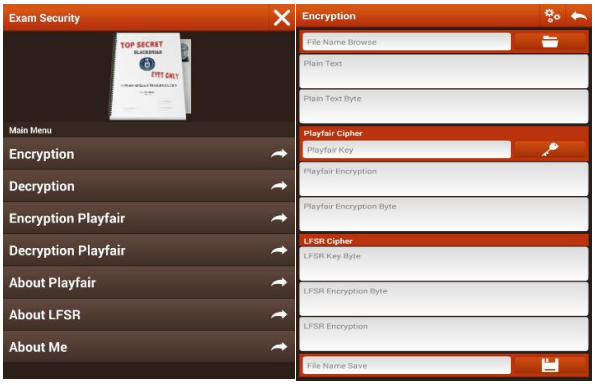


Figure IV-1 *Main Interface Application and Encryption*

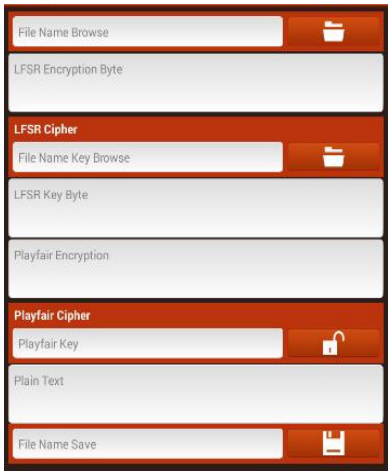


Figure IV-2 Interface Description

B. ***The results of the 13x13 Playfair Cipher Matrix Cryptography Test and merged with LFSR***

In the test of ciphertexst randomness is done as much as 30 experiments with different sample parameters that is based on the size of the file, the length of ciphertext characters and the same key. Results obtained from experiments using the application is calculated using the Avalanche Effect method with the formula :

$$\textit{Avalanche Effect} = \frac{\text{jumlah perubahan bit}}{\text{jumlah seluruh bit chiperteks}} \text{ x } 100\%$$

Where the number of bit changes obtained from the results of XOR calculation between plaintext with ciphertext first converted into binner number, then to prove that the modification of playfair algorithm with 13x13 key matrix and combined with LFSR have higher value of ciphertext randomness, then made comparison with previous method . Here is the result of the comparison of ciphertext randomness test can be seen in Table IV-1 :

Table IV-1 *Comparison of Ciphertext Randomness Test Results*

No	Name Data/File	Plaintext length (bit)	*Avalanche Effect*		
			Playfair 5x5	Playfair 10x10	Playfair 13x13 & LFSR
1	Ujicoba1	112	26,79	31,25	40,18
2	Ujicoba2	472	30,93	35,17	41,31
3	Ujicoba3	943	28,74	33,19	45,07
4	Ujicoba4	1247	29,35	34,64	41,06
5	Ujicoba5	1.961	29,73	35,90	46,51
6	Ujicoba6	2.232	32,21	32,39	39,87
7	Ujicoba7	3.480	31,75	33,33	45,34
8	Ujicoba8	3.680	31,30	36,88	47,31

No	Name Data/File	Plaintext length (bit)	*Avalanche Effect*		
			Playfair 5x5	Playfair 10x10	Playfair 13x13 & LFSR
9	Ujicoba9	4.224	32,15	36,65	44,96
10	Ujicoba10	5.320	32,05	33,59	45,15
11	Ujicoba11	5.904	32,57	36,26	46,93
12	Ujicoba12	6.816	32,42	31,41	45,77
13	Ujicoba13	7.872	31,40	35,71	41,92
14	Ujicoba14	8.376	31,40	33,82	45,01
15	Ujicoba15	18.696	31,61	33,62	45,97
16	Ujicoba16	10.840	39,18	30,50	38,81
17	Ujicoba17	16.480	40,18	29,78	43,62
18	Ujicoba18	12.176	39,38	28,56	45,43
19	Ujicoba19	31.592	38,17	30,82	44,94
20	Ujicoba20	19.440	38,11	30,95	39,61
21	Ujicoba21	33.472	38,18	29,24	40,14
22	Ujicoba22	35.896	37,09	30,74	39,96
23	Ujicoba23	25.592	36,42	31,06	44,40
24	Ujicoba24	38.600	36,67	30,33	44,80
25	Ujicoba25	58.256	37,72	30,09	44,48
26	Ujicoba26	70.112	37,25	29,91	40,10
27	Ujicoba27	95.880	37,21	29,32	44,73
28	Ujicoba28	121.648	37,21	29,35	39,49
29	Ujicoba29	138.880	37,80	29,76	44,15
30	Ujicoba30	141.368	37,37	30,26	44,63
Average *Avalanche Efect*			**34,41**	**32,15**	**43,39**

C. ***Time* Complexity Testing**

In this time complexity testing done 30 times experiment with different sample parameters that is based on the size of the file and the length of the character ciphertext. This time complexity testing is obtained from the application during encryption process and description. After that done the average calculation time of encryption and description. Here is the result of time complexity test between Playfair 13x3 key matrix and merged with LFSR, Playfair classic martick lock 5x5 and Playfair 10x10 key matrix can be seen in Figure IV-3, Figure IV-4. Figure IV-5 and Figure IV-6 :

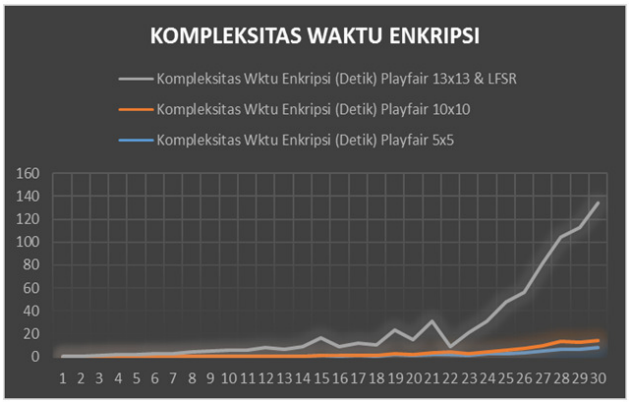


Figure IV-3 Complexity of Encryption Time

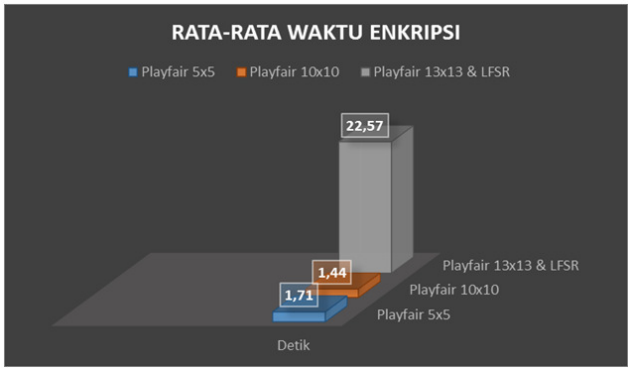


Figure IV-4 Average Encryption Time

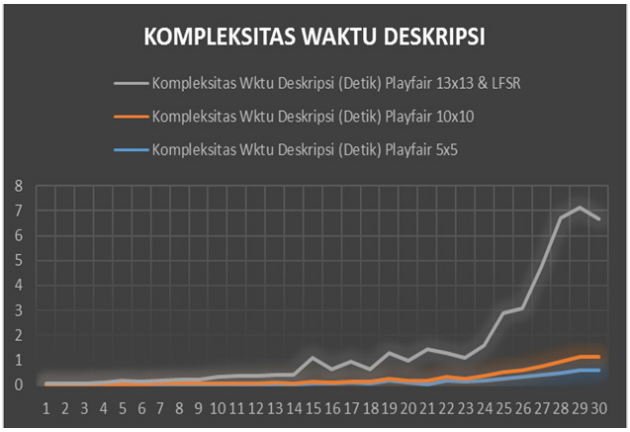


Figure IV-5 Complexity Time Description

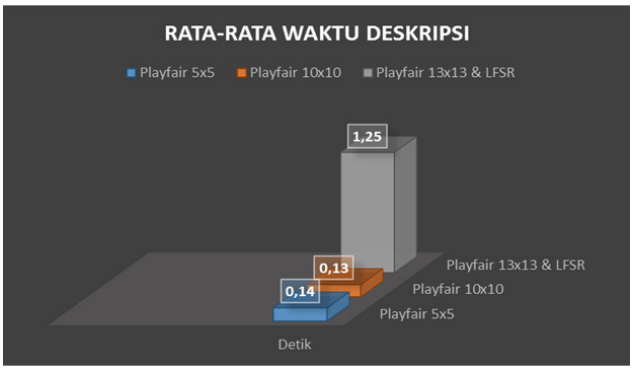


Figure IV-6 Average Time Description

V. CONCLUSIONS

Based on the research that has been done, this cryptographic technique can answer the hypothesis at the beginning of the research that is the modification of playfair method with 13 x 13 table and combined with linear feedback Shift Register (LFSR) 8 bit, can improve the previous playfair deficiency such as, by changing the size of the matrix key 13x13 then playfair cipher able to insert

characters as much as 196 characters consisting of capital letters, lowercase letters, numbers and some symbols. The result of avalanche effect calculation is got the mean value of playfair cipher algorithm done by modification of 13x13 matrix key and combined with LFSR generator 43.59%, playfair cipher algorithm performed 10x10 matrix modification without merged with LFSR of 32.15% and classical playfair algorithm 5x5 matrix without combined with LFSR of 34.41%.

This shows that the playfair cipher algorithm with 13x13 matrix and combined with the LFSR generator has a more random ciphertext than the previous playfair cipher and it can be concluded that the modified playfair cipher and combined with the LFSR generator is stronger than the previous playfair cipher, making it more difficult cryptanalysis in analyzing the bigram. Time stamp counter (TSC) time encryption test results obtained 22.57 seconds encryption time average on Playfair 13x13 method combined with LFSR, 1.44 sec on 10x10 Playfair method and 1.71 seconds on classical Playfair 5x5 method, while the average descriptions time of 1.25 seconds on the 13x13 Playfair method combined with LFSR, 1.13 seconds on the Playfair 10x10 and 1.14 sec methods on the classical 5x5 Playfair method. The value of the 13x13 Playfair method combined with LFSR is even greater than the Playfair 10x10 and Playfair 5x5 methods but the three methods are classified as having fast encryption and decryption times.

REFERENCES

[1] K. Bhat, D. Mahto, and D. K. Yadav, "Vantages of Adaptive Multidimensional Playfair Cipher over AES-256 and RSA-2048," vol. 8, no. 5, pp. 2015–2017, 2017.

[2] K. Bhat, D. Mahto, and D. K. Yadav, "a Novel Approach To Information Security Using Four Dimensional (4D) Playfair Cipher Fused With Linear," vol. 8, no. 1, pp. 15–32, 2017.

[3] Nurkifli, E. H. (2014). Modifikasi Algoritma Playfair dengan matriks 12x12, (Sentika).

[4] H. Tunga and S. Mukherjee, "A New Modified Playfair Algorithm Based On Frequency Analysis," vol. 2, no. 1, 2012.

[5] J. Choudhary, R. Kumar Gupta, and S. Singh, "a Generalized Version of Play Fair Cipher," *Compusoft*, vol. 2, no. 6, pp. 176–179, 2013.

[6] E. Andriana and E. Andriana, "Algoritma Enkripsi Playfair Cipher Algoritma Enkripsi Playfair Cipher," no. May, pp. 0–5, 2016.

[7] R. W. Simbolon, "Cipher Dan Steganografi Dengan Teknik Least Significant Bit (Lsb) Protecting The Student Academic Transcript Using Playfair Cipher Cryptography," vol. 5, no. 1, pp. 59–70, 2016.

[8] G. H. Ekaputri, "Super-Playfair , Sebuah Algoritma Varian Playfair Cipher dan Super Enkripsi."

[9] T. Nafis, M. Sadiq, and N. Siddiqui, "Addendum of Playfair Cipher in Hindi," vol. 10, no. 5, pp. 977–983, 2017.

[10] I. Pomeranz, "LFSR-Based Generation of Multicycle Tests," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 70, no. c, pp. 1–1, 2016.