ANDROID DATA SECURITY USING CRYPTOGRAPHIC ALGORITHM COMBINATIONS

April Lia Hananto[1,] Bayu Priyatna[2], Ai Rosita[3]

Abstract---*Android is a platform that is very vulnerable to hacked by bad people to steal users' data intentionally or unintentionally [1]. To deal with data disturbances it is necessary to use cryptography [2], one of which is Playfair Chipper. Playfair's cryptographic algorithms are currently being developed with various types of matrix table modifications, ranging from changes in matrix size, or changes in the encryption process steps. The results of applying the Playfair combination and modification algorithm with the Linear Feedback Ship Register (LFSR) for securing data on the Android platform. Testing the application of the results of the Playfair algorithm modification using the Avalanche Effect can be concluded that the resulting ciphertext has a high complexity.*

Keywords---*Android, LFSR, playfair cipher, modification, cryptography.*

I. INTRODUCTION

The increase in applications utilizing the Android platform is felt to help provide benefits in various fields; both social, health, and government. But it needs to be reminded that the Android platform has an open-source that can support software developers to exploit traces of digital applications, and Android is also a platform that is very vulnerable to be hacked by bad guys for personal data [1].

To deal with data disturbances, it is necessary to use cryptography [2], one of them is Playfair Chipper. Playfair's cryptographic algorithms are currently being developed with various types of matrix table modifications, ranging from changes in matrix size, or changes in the encryption process steps. Also, combining with other cryptographic techniques can be done, with the hope of being able to strengthen the security of the data from the encryption process, and produce a complex ciphertext that is difficult to solve [3].

Various assault techniques such as; Known Plaintext Attack, Brute Force Attack, and Frequency Analysis can be handled well [4]. In this paper, we test the application of the results of the matrix modification, encryption process and combining with the Linear Feedback Ship Register (LFSR) algorithm for securing data on the Android platform, as well as testing the resulting ciphertext complexity.

[1,2] Information Systems Study Program
School of Engineering and Computer Science
Universitas Buana Perjuangan Karawang
[3]Widyatama University
[1] Email: aprilia@ubpkarawang.ac.id
[2] Email: bayu.priyatna@ubpkarawang.ac.id
Ai.rosita@widyatama.ac.id

II. THEORETICAL BASIS

Cryptography

It is a technique of deception sentences so that the original meaning cannot be known. Now cryptography is no longer limited to encrypting messages but can also prepare security aspects against attacks from cryptanalysis. Therefore, the idea of cryptography also turned into science and art to maintain message security [10]. Cryptography is a process used to help improve data security [5].

Classic Method of Playfair Cipher Cryptography

Symmetrical key substitutions are often mentioned in the Playfair Chipper method. The technique used in conventional Playfair cipher divides the plaintext into sets of two-letter and number characters, each known as a digraph consists of the alphabet as identification. Playfair algorithm that uses a 5X5 matrix with 25 letters [6], made as in Figure II-1. The key table used for the encryption and decryption process is made placing key letters without repetition from left to right and from top to bottom in the matrix table, then the remaining matrices are equipped with the remaining letters in alphabetical order. And change the letter "J" to "I" if it's in the plaintext [11].

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 [11].

Classic Playfair Cipher Encryption Algorithm

The following are the steps and rules that exist in Playfair Chipper:

1. Arrange plaintext characters into paired matrices (2 x n)
2. Characters and spaces that may not be in the plaintext (if any) must be replaced first.
3. Plaintext Being the original message is carried out by the letter pairs (bigram).
4. If the letter J is available in the plaintext, replace it with the character letter I. as shown in figure II-2:

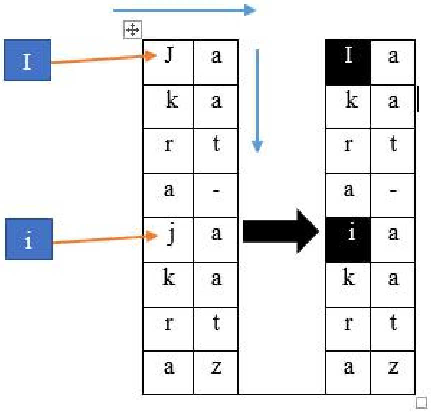

Figure II-2 Plaintext in pairs

1. When there are the same pair of characters, then change one letter of the letter pair with the letter Z or X enter it using the letter X because the letter X is very minimal in the same bigram, unlike the letter Z, for example, is the word PASSWORD.

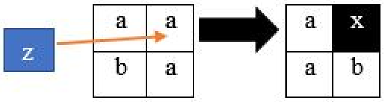

Figure II-3 Plaintext With the Same Pair

2. If there are letters in the unpaired plaintext then select additional letters then add at the end of the plaintext. Additional letters can be selected, for example, the letter Z or X [7].

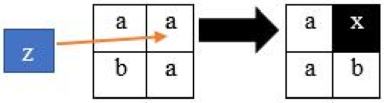

Figure II-4 Plaintext not in pairs

Description Plafair Cipher

At the stage of return or Decryption Playfire has the following stages:

1. If there are two letters on the same key line, then each letter is changed using the letters on the left.
2. If there are two letters in the same column, then each letter is changed by the letters above it.
3. If the two letters are not on the same row and column, change to the letter at the intersection of the first row with two-column letters. Then the second letter is then changed using the letter in the fourth vertex of the rectangle formed from the letter used [12].

Linear Feedback Shift Register (LFSR)

Generator Linear Feedback Shif Register (LFSR) [8]. Is a register that can shift with a certain number of conditions, the final result will be selected and added two modulo, then return to the input register at each clock cycle. LFSR has an N storage element called stages. The n-stage LFSR is flagged by an n × n matrix, called TSR, a size format based on the feedback stage dependency. Furthermore, the state is a linear function of the previous state [13]. A shift in the linear feedback register (LFSR) is needed to produce the key given to the encryption and decryption block [9].

III. SYSTEM DESIGN

The security design must be able to provide end-to-end authentication, message confidentiality, and integrity [10]. The model used in this study is a technique, by changing the steps of the encryption algorithm, modifying the table using a 13 x 13 matrix and combining it with an 8-bit Linear Feedback Shift Register (LFSR) [11]. The process flow of this research is outlined in Figure III-1 as follows:

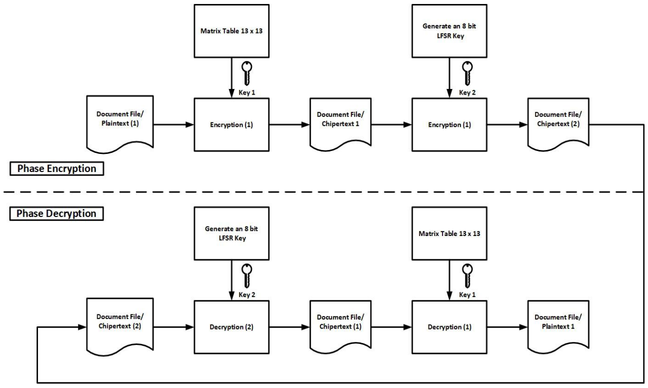
Matrix Table 13 x 13
Generate an 8 bit LFSR Key
Key 1
Key 2
Document File/ Plaintext (1)
Encryption (1)
Document File/ Chipertext 1
Encryption (1)
Document File/ Chipertext (2)
Phase Encryption
Phase Decryption
Generate an 8 bit LFSR Key
Matrix Table 13 x 13
Key 2
Key 1
Document File/ Chipertext (2)
Decryption (2)
Document File/ Chipertext (1)
Decryption (1)
Document File/ Plaintext 1

Figure III-1 Flow of Data Security System

Playfair 13 x13 Matric

Formation of a 13 x 13 matrix key Playfair matrix is included, in the formation of a key consisting of letters, numbers, and symbols. The first step is that a key consisting of a combination of characters must not have more than one appearance if there is such a thing then delete numbers, letters or symbols that have similarities. So the key "D4wn4tt @ ck" becomes "D4wnt @ ck". In Table III-2 is a matrix formed by the key "D4wnt @ ck":

D	4	w	n	t	@	c	k	A	B	C
E	F	G	H	I/J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X	Y	Z	a
b	d	e	f	g	h	i/j	l	m	o	p
q	r	s	u	v	x	y	z	0	1	2
3	5	6	7	8	9	~	!	#	$	%
^	&	*	(	)	_	+	=	-	<	>
"	,	.	«	ª	\	?	`	β	γ	ε
ɰ	€	≠	©	¶	¼	Í	√	Œ	™	•
ª	¦	Ö	Û	à	ò	ó	ô	»	µ	±
®	ø	æ	µ	°	¨	’	‘	Ž	†	‡
Þ	½	¾	Ù	Ú	Ü	Ý	ã	ä	å	î
ï	ð	¿	¯	¡	¤	¬	™	‰	÷	|

Figure III-2 Key Matrix Modification on Playfair

Linear Feedback Shift Register (LFSR)

The step in the data encryption method uses 16-bit Shift Register (LFSR) linear feedback, which will form a key matrix. The following is an illustration of the key formation process of the key from LFSR:

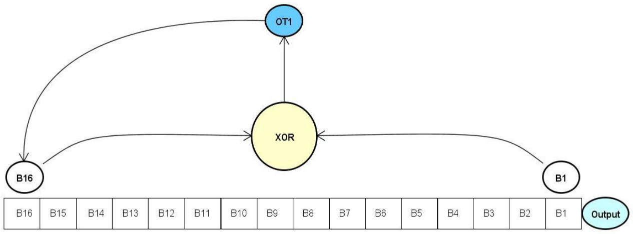

Figure III-3 Key Formation Process

In Illustration Figure III-3 is a depiction of flow in key formation with 16-bit LFSR. Where B16, B15,... B1 represents B16 xor B1 input bits then B1 is shifted and placed in the output bits. Figure III-4 is the result of the LFSR key development process:

B16	B15	B14	B13	B12	B11	B10	B9	B8	B7	B6	B5	B4	B3	B2	B1	Output
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	-
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1
0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1
0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0
1	1	1	1	1	0	0	0	0	0	0	0	1	0	0	0	0
1	1	1	1	1	1	0	0	0	0	0	0	0	1	0	0	0
1	1	1	1	1	1	1	0	0	0	0	0	0	0	1	0	0
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1	0

Figure III-4 Establishment of LFSR Keys

In figure III-4 the initial input is 0000000100000011 then the result obtained is 1100000010000000 then the next output is continued up to (n). Then the resulting output is compiled with a size matrix (2 × n) where the length (n) is based on the length of the line contained in the ciphertext that has been generated from the encryption process 1, using the Playfair cipher. The output of the bits will be converted to decimal and the decimal obtained will be converted to the equivalent ASCII character [12].

IV. RESULT AND DISCUSSION

Implementation on the Android Platform

Android application interface that is built can be seen in Figure IV-1 and Figure I:

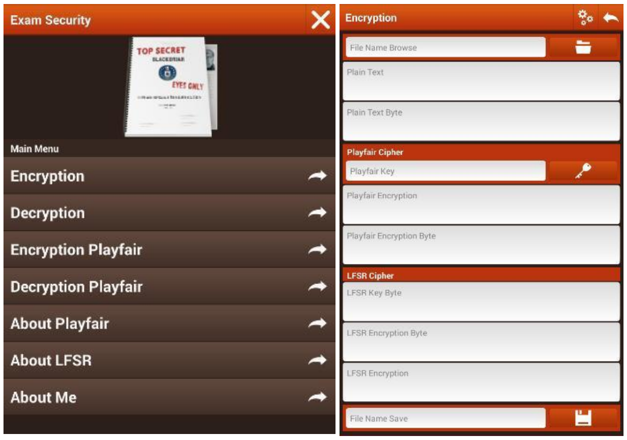

Figure IV-1 Data Encryption Android Application

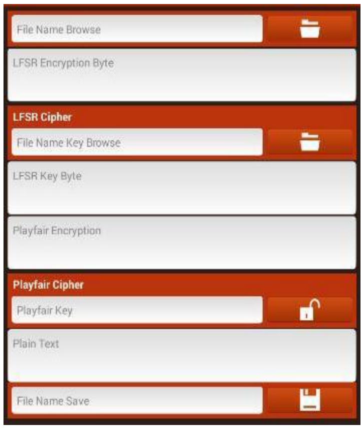

Figure IV-2 Data Decription Android Application

Ciperteks Randomness Test

In the ciphertext randomness test, 30 trials were performed with random sample parameters based on the same data size, character length, and key. The results of the experiment using the calculation of the Avalanche Effect method with the formula:

$$\boldsymbol{Avalanche\ Effect} = \frac{\text{number of bit changes}}{\text{the total number of chipload bit}} \text{ x } 100\% \qquad (4.1)$$

Generally, the bits in the ciphertext will change from the number of bits in the plaintext by 50%. Avalanche effect is said to be good if the resulting bit change ranges from 45-60% (about half). The more bit changes that occur cause the more difficult the cryptographic algorithm to solve or have high complexity [14]. Implementation of the Avalanche Effect the number of bit changes obtained from XOR calculations between plaintext and ciphertext is converted to binner numbers, then prove that the modified Playfair algorithm combined with LFSR has a higher ciphertext randomness value. The following is the result of the comparison of the ciphertext randomness test which can be seen in Table IV-1 and Figure IV-4 Graph of Avalanche Effect:

Table IV-1 Comparison of Ciphertext Randomness Test Results

No	Data / File Name	Plaintext length (bit)	Afvalanche Effect
1	Sample 1	142	40,18
2	Sample 2	482	41,31
3	Sample 3	993	45,07
4	Sample 4	1287	41,06
5	Sample 5	1.981	46,51
6	Sample 6	2.212	40,87
7	Sample 7	3.580	45,34
8	Sample 8	3.780	47,31
9	Sample 9	4.324	44,96
10	Sample 10	5.520	45,15
11	Sample 11	5.804	46,93
12	Sample 12	6.916	48,77
13	Sample 13	7.882	41,92
14	Sample 14	8.576	45,01
15	Sample 15	18.796	45,97

No	Data / File Name	Plaintext length (bit)	Afvalanche Effect
16	Sample 16	10.940	38,81
17	Sample 17	16.980	43,62
18	Sample 18	12.176	45,43
19	Sample 19	31.992	44,94
20	Sample 20	19.840	39,61
21	Sample 21	33.372	40,14
22	Sample 22	35.796	39,96
23	Sample 23	25.692	44,40
24	Sample 24	38.680	44,80
25	Sample 25	58.286	44,48
26	Sample 26	70.212	40,10
27	Sample 27	95.890	44,73
28	Sample 28	121.748	44,49
29	Sample 29	138.780	44,15
30	Sample 30	141.468	44,63

No	**Data / File Name**	**Plaintext length (bit)**	**Afvalanche Effect**
Avalanche Effect Average Score			**43,69**

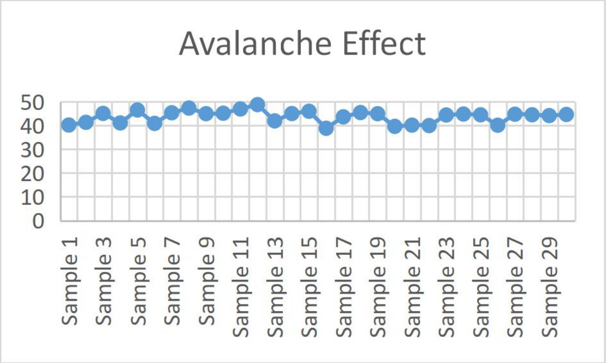

Figure IV-3 Avalanche Effect graph

V. CONCLUSIONS

Based on the results of research conducted, data security on Android can answer the hypothesis at the beginning of the research by implementing the Playfair algorithm and then combining it with 16-bit Shift Register (LFSR) linear feedback, which can increase the lack of data security on the previous Android such as, by changing the key size matrix 13x13, the Playfair cipher can insert 196 characters consisting of capital letters, lowercase letters, numbers, and symbols, then the results of the ciphertext randomness effect test of avalanches obtained an average value of the Playfair algorithm 43.69%. so, it is increasingly not easy to be attacked with the techniques of Plaintext Attack, Bruteforce Attack, and Frequency Analysis.

VI. RECOMMENDATION

This result will be much better if implemented on the data communication system protocol of the Android platform. The combination of the Playfair algorithm using asymmetric methods, such as RSA or AES is expected to be able to provide changes to the ciphertext that is produced much better.

REFERENCES

[1] O. Ahmed and A. Sallow, “Android Security: A Review,” *Acad. J. Nawroz Univ.*, vol. 6, no. 3, pp. 135–140, 2017.

[2] F. De Rango, G. Potrino, M. Tropea, and P. Fazio, “Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks,” *Pervasive Mob. Comput.*, vol. 61, p. 101105, 2020.

[3] D. Atmodjo, “Peningkatan Keamanan Data dengan Metode Cropping Selection Pseudorandom,” vol. 4, no. 3, pp.

132–138, 2016.

[4] S. C. St and A. N. St, “A Comprehensive Study on Security issues in Android Mobile Phone — Scope and Challenges A Comprehensive Study on Security issues in Android Mobile Phone Scope and Challenges,” *Int. J. Innov. Res. Adv. Eng.*, vol. 3, no. JANUARY, pp. 62–72, 2016.

[5] N. Indira, S. Rukmanidevi, and A. V Kalpana, “Light Weight Proactive Padding Based Crypto Security System in Distributed Cloud Environment,” pp. 1–9, 2019.

[6] H. B. Habib and H. B. Habib, “Diyala Journal for Pure Science,” no. 4, pp. 74–84, 2019.

[7] D. Kurniawan, A. L. Hananto, and B. Priyatna, “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,” *Int. J. Comput. Tech. -*–, vol. 5, no. 1, pp. 65–70, 2018.

[8] S. Dutta and A. Chakraborty, *A Deep Learning-Inspired Method*. Springer Singapore, 2019.

[9] S. Karunamurthi and V. Krishnasamy Natarajan, “VLSI implementation of reversible logic gates cryptography with LFSR key,” *Microprocess. Microsyst.*, vol. 69, pp. 68–78, 2019.

[10] G. Srivastava, R. Agrawal, K. Singh, R. Tripathi, and K. Naik, “A hierarchical identity-based security for delay tolerant networks using lattice-based cryptography,” *Peer-to-Peer Netw. Appl.*, 2019.

[11] M. I. Fitrianda, *Digital Digital Repository Repository Universitas Universitas Jember Jember Digital Digital Repository Repository Universitas Universitas Jember*. 2013.

[12] R. M. Marzan, A. M. Sison, and R. P. Medina, “Randomness analysis on enhanced key security of Playfair cipher algorithm,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 4, pp. 1248–1253, 2019.

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

[14] Prakash, G., Darbandi, M., Gafar, N., Jabarullah, N.H., & Jalali, M.R. (2019) A New Design of 2-Bit Universal Shift Register Using Rotated Majority Gate Based on Quantum-Dot Cellular Automata Technology, International Journal of Theoretical Physics, https://doi.org/10.1007/s10773-019-04181-w..

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

[16] 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.

[17] Sugiyanto, Rinci Kembang Hapsari. (2016). Pengembangan Algoritma Advanced Encryption Standard pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere. Surabaya, ISSN 2085-4552

Biography

1. April Lia Hananto
2. Lecturer
3. University of Buana Perjuangan Karawang
4. Jl HS. Ronggo Waluyo, Telukjambe Timur, Kabupaten Karawang,
   Jawa Barat 41361
5. Email : aprilia@ubpkarawang.ac.id

Biography: (Only 50 words)

....

....

....

1. Bayu Priyatna
2. Lecturer
3. University of Buana Perjuangan Karawang
4. Jl HS. Ronggo Waluyo, Telukjambe Timur, Kabupaten Karawang,
   Jawa Barat 41361
5. Email : bayu,priyatna@ubpkarawang.ac.id

Biography: (Only 50 words)

....

....

....