PENGAMANAN DATA BERBASIS MOBILE ANDROID DENGAN PENGGABUNGAN LINEAR FEEDBACK SHIFT REGISTER (LFSR) DAN MODIFIKASI MATRIKS KUNCI ALGORITMA KRIPTOGRAFI PLAYFAIR CIPHER

Denni Kurniawan[1], Bayu Priyatna[2]

[1)]Program Studi Magister Ilmu Komputer, Program Pascasarjana, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Pesanggrahan, Jakarta Selatan 12260
Telp. (021) 595753, Fax. (021) 5869225
[2)] Universitas Buana Perjuangan Karawang
Jalan HS. Ronggo Waluyo, Telukjambe Timur, Puseurjaya, Telukjambe Timur, Kabupaten Karawang
Telp. (0267)8403140
[1]*d3nni.k0@gmail.com*, [2]*bayu.priyatna20@gmail.com*

ABSTRAK

Playfair cipher merupakan metode enkripsi klasik yang sulit untuk dikriptanalisis secara manual namun selain dari kelebihan yang terdapat pada plyafair cipher terdapat juga banyak kekurangan diantaranya, dapat dipecahkan dengan menggunakan informasi frekuensi kemunculan bigram, tidak dapat memasukkan huruf kecil, angka dan karakter khusus pada saat melakukan enkripsi.. Penelitian ini melakukan modifikasi pada matriks kunci algoritma kriptografi playfair dan menggabungkan dengan algoritma Linear Feedback Shift Register (LFSR), dengan merubah ukuran matriks kunci 13x13 maka playfair cipher mampu menyisipkan karakter sebanyak 196 karakter terdiri dari huruf kapital, huruf kecil. Hasil perhitungan dengan metode avalanche effect didapatkan nilai rata-rata 43,59% pada playfair cipher yang dilakukan modifikasi kunci matriks 13x13 dan digabung dengan generator LFSR, 2,15% pada playfair cipher kunci matriks 10x10 tanpa digabung dengan LFSR dan 34,41% pada playfair klasik 5x5. Bahwa playfair cipher yang telah dimodifikasi dan digabung dengan generator LFSR ini lebih kuat dari playfair cipher sebelumnya. Hasil pengujian kompleksitas waktu memiliki enkripsi dan dekripsi yang cepat.

Kata Kunci: *Playfair*, LFSR, kriptografi, enkripsi, deskripsi.

I. PENDAHULUAN

Data akan menjadi penting jika menghasilkan informasi yang bermanfaat bagi seseorang maupun suatu lembaga atau perusahaan, pada umumnya informasi yang penting akan selalu menghasilkan validasi yang bernilai tinggi sesuai dengan prinsip dari informasi sendiri yaitu dapat dipercaya keasliannya dan jelas keberadaan sumbernya. Tidak menutup kemungkinan bahwasanya informasi yang sangat penting dan memiliki nilai yang tinggi dapat menjadi target sasaran para pelaku tindak kejahatan, yang memang dengan sengaja ingin memanfaatkan kelemahan yang terdapat pada sistem baik konvensional maupun modern seperti pencurian dan perusakan data. Adapun teknik yang dapat digunakan untuk menjaga isi dari sebuah data sangatlah bermacam-macam salah satunya adalah dengan menggunakan teknik Kriptografi *(Chryphtography)*. Kriptografi sendiri berasal dari bahasa Yunani yaitu *"cryptós"* yang artinya rahasia, sedangkan "gráphein" artinya tulisan, sehingga jika digabungkan menjadi "tulisan rahasia". Saat ini kriptografi sering digunakan pada banyak hal terutama untuk menjaga keamanan informasi seperti kerahasiaan/privasi *(confidentiality/privacy)*, integritas data *(dataintegrity),* otentikasi (authentication), dan tanpa penyangkalan (nonrepudiation) yang digunakan untuk pembuktian (Simbolon, 2016). Contoh teknik kriptografi yang digunakan baik klasik maupun moderen, diantaranya adalah, *Vigenere, Playfair,* AES, RSA dan masih banyak yang lainnya. Menurut Bhat [1], Hasil analisa perbandingan antara kriptografi AES, RSA dan *Playfair Cipher*, bahwa *Playfair Cipher* unggul dalam mengamankan data secara efisien dan tidak ambigu. Menurut Mahyudin [2], *Playfair Cipher* sebaiknya digunakan untuk menyamarkan pesan penting yang dibutuhkan secara cepat.

Kemudian [3], Playfair Cipher merupakan metode enkripsi klasik yang sulit untuk dikriptanalisis secara manual. Komponen yang penting pada algoritma playfair adalah tabel cipher yang digunakan untuk melakukan enkripsi dan dekripsi tabel bawaan yang diperkenalkan oleh playfair adalah tabel yang memiliki bentuk matriks berukuran (5x5) yang berisi huruf kapital dari A-Z dengan menghilangkan huruf J. Meskipun pengamanan teks pada algoritma Playfair cipher ini sangat sulit untuk dikripanalisis, akan tetapi masih dapat dipecahkan dengan menggunakan informasi frekuensi kemunculan bigram.

Selain permasalahan tersebut [4], pada algoritma *Playfair cipher* klasik masih terdapat sejumlah kelemahan seperti tidak bisa memasukkan huruf kecil, angka dan karakter khusus pada saat melakukan enkripsi. *Ciphertext* yang dihasilkan algoritma playfair mudah sekali dipecahkan ketika seorang kriptanalisis mengetahui ciphertext dan tabel cipher-nya, walaupun kriptanalis hanya mengetahui ciphertext-nya saja tanpa harus mengetahui tabel chiper kriptanalis dapat menebak bigram berdasakan huruf yang bermakna dari sebuah kata [5].

Walaupun dengan melakukan modifikasi isi bujur sangkar kunci hanya dengan menggeser sesuai banyaknya kolom, maka sebetulnya kunci yang dihasilkan berulang setiap 5 kali. Dengan demikian ini akan menghasilkan celah untuk melakukan kriptanalisis [6].

Melihat dari faktor permasalahan tersebut, penulis tertarik untuk melakukan modifikasi pada matriks kunci algoritma kriptografi *Playfair* dan menggabungkan dengan algoritma kriptografi lain, kemudian menerapkan algoritma kriptografi *Playfair* yang sudah modifikasi tersebut ke-dalam bentuk program aplikasi dan diterapkan untuk pengamanan sebuah data.

II. LANDASAN TEORI

2.1. Kriptografi / *Cryptography*

Kriptografi *(cryptography*) di dalam bahasa Yunani terbagi menjadi dua istilah yakni "cryptós" yang memiliki arti rahasia, sedangkan "gráphein" artinya tulisan, dari kedua istilah tersebut digabungkan sehingga menjadi "tulisan rahasia"[7]. Awal mulanya kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikan kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Kemudian seiring dengan perkembangannya kriptografi tidak lagi sebatas mengenkripsikan pesan, tetapi juga memberikan aspek keamanan terhadap serangan dari kriptanalisis. Karena itu pengertian kriptografipun berubah menjadi ilmu sekaligus seni untuk menjaga keamanan pesan [8].

2.2. Kriptografi Playfair Cipher

Playfair Cipher adalah kunci substitusi substitusi simetrik kunci simetris.Teknik yang digunakan dalam playfair cipher konvensional memecah *plaintext* dalam beberapa set dari dua karakter yang masing-masing dikenal sebagai digraphs. Yaitu adalah terdiri dari abjad sebagai identifikasi. Algoritma sandi Playfair dibentuk dengan menggunakan matriks 5 × 5 dari 25 huruf yang dibuat seperti ditunjukkan pada gambar II-1. Matriks kunci yang diperlukan untuk proses enkripsi dan deskripsi dibangun dengan menempatkan huruf-huruf dari kata kunci tanpa pengulangan dari kiri ke kanan dan dari atas ke bawah dalam matriks, dan kemudian sisa matriks selesai dengan abjad yang tersisa dalam urutan alfabet. Dan merubah huruf "J" menjadi "I" jika terdapat pada *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

Gambar 1 : Contoh Matriks Kunci [9].

2.2.1. Algoritma Enkripsi *Playfair Cipher*

Sebelum melakukan proses enkripsi, plaintext yang akan dilakukan enkripsi diatur terlebih dahulu sebagai berikut :

1. Semua karakter dan spasi yang bukan termasuk alfabet harus dihilangkan terlebih dahulu dari plaintext (jika ada).
2. Jika terdapat huruf J pada plaintext lakukanlah perubahan dengan huruf I.
3. Plaintext yang menjadi pesan asli dilakukan penyusunan sesuai pasangan huruf (bigram).
4. Ketika terdapat pasangan huruf yang sama maka lakukan perubahan salah satu huruf dari pasangan huruf dengan huruf Z atau X sisipkanlah dengan menggunakan huruf X karena huruf X sangat minim sekali sama dalam bigram, tidak seperti pada huruf Z, contohnya adalah pada kata FUZZY.
5. Jika huruf pada plaintext memiliki jumlah ganjil maka pilih huruf tambahan kemudian tambahkan di akhir plaintext. Huruf tambahan dapat dipilih misalnya huruf Z atau X.

2.2.2. Algoritma Deskripsi *Plafair Cipher*

Berikut merupakan tahapan dari algoritma playfair cipher :

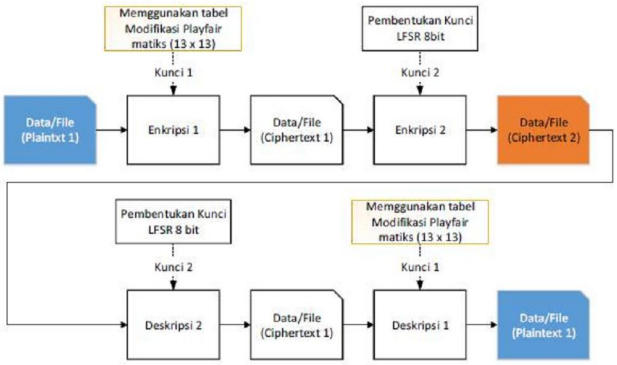
1. Jika terdapat dua huruf yang terletak pada baris kunci sama maka setiap huruf diubah menggunakan huruf di kirinya.
2. Jika terdapat dua huruf yang terletak pada kolom yang sama maka setiap huruf diubah dengan huruf di atasnya.
3. Jika terdapat dua huruf tidak berada pada baris dan kolom yang sama, maka ubahlah dengan huruf yang terdapat pada perpotongan baris huruf yang pertama dengan kolom huruf dua. Kemudian berikutnya huruf kedua diubah menggunakan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf yang digunakan [3].

2.3. *Linear Feedback Shift Register (LFSR)*

LFSR adalah register yang bergeser dengan jumlah tertentu, output dipilih dan ditambahkan modulo 2. Selain itu diumpankan kembali ke register input pada setiap clock cycle. LFSR sendiri terdiri dari elemen penyimpanan N yang disebut tahapan. Sebuah N-stage LFSR ditandai dengan matriks N × N, yang disebut dengan TSR. Format dan ukurannya TSR didasarkan pada ketergantungan umpan balik tahap. Selanjutnya, state adalah fungsi linier dari keadaan sebelumnya [10].

III.RANCANGAN SISTEM DAN APLIKASI

Metodologi penelitian yang digunakan dalam penelitian ini adalahrekayasa, yaitu Theoretical Computer Science dimana peneliti menggunakan suatu teknik kriptografi dengan metode modifikasi tabel algoritma playfair menggunakan matriks 13x13 dan menggabungkannya dengan Linear Feedback Shift Register (LFSR) 8 bit, Adapun gambaran alur sistematika proses dari penelitian ini dituangkan dalam gambar III-1 sebagai berikut :



Gambar 2 : Alur Sistem Pengamanan Data

3.1. Matiks Playfair 13x13

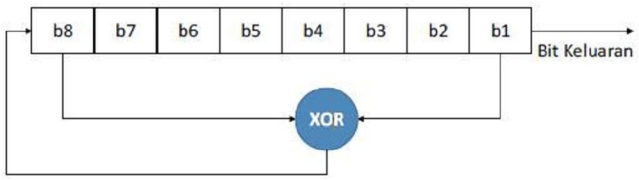
Pembentukan tabel matriks playfair 13 x 13 dari kunci yang telah dimasukan, pada pembentukan kunci yang terdiri dari huruf, angka dan simbol Misalkan contoh kunci "AkuM@Ululu5". Langkah yang pertama adalah kunci yang terdiri dari angka, huruf atau simbol tidak boleh memiliki kemunculan lebih dari satu jika terdapat hal tersebut maka hilangkan angka, huruf atau simbol yang memiliki kesamaan. Sehingga kunci dari "AkuM@Ululu5" menjadi "AkuM@Ul5". Pada Tabel III-2 adalah matriks yang terbentuk dari kunci "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	#	∞	±	≥	≤	{
÷	{	}	Ä	Å	È	É	Ë	Ê	Ì	Í	Î	}
Ï	Đ	Ñ	Ò	Ó	Ô	Õ	Ö	Ø	Ù	Ú	Û	!
Ý	À	á	â	ä	Å	Ω	Ç	è	É	ê	ë	⌠
ì	Í	î	ï	ð	Ñ	ò	Ó	ô	Õ	ù	⌂	$
₹	⌉	Σ	≠	ğ	€	Ω	λ	Ľ	Đ	Ï	Ý	┤

Gambar 3: Matriks 13x13 Playfair

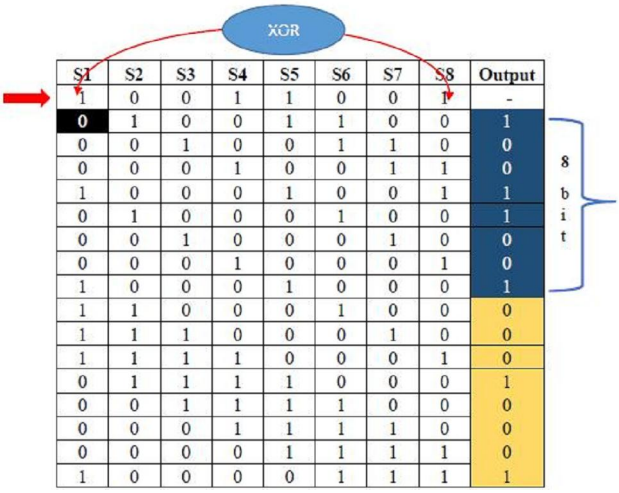
3.2. Pembentukan Matriks Kunci *Linear Feedback Shift Register (LFSR)*

Langkah dalam metode enkripsi data menggunakan linear *feedback Shift Register (LFSR) 8 bit,* adalah pembentukan matriks kunci. Berikut adalah ilustrasi proses pembentukan kun kunci LFSR :



Gambar 4: Proses Pembentukan Kunci

Pada ilustrasi gambar di atas menjelaskan mengenai tahapan atau alur proses dalam pembentukan kunci dengan LFSR 8 bit. Dimana b1, b2, ...b8 merupakan suatu bit masukan b1 xor b8 kemudian b8 digeser dan ditempatkan di bit keluaran. Berikut adalah hasil dari proses pembentukan kunci LFSR :



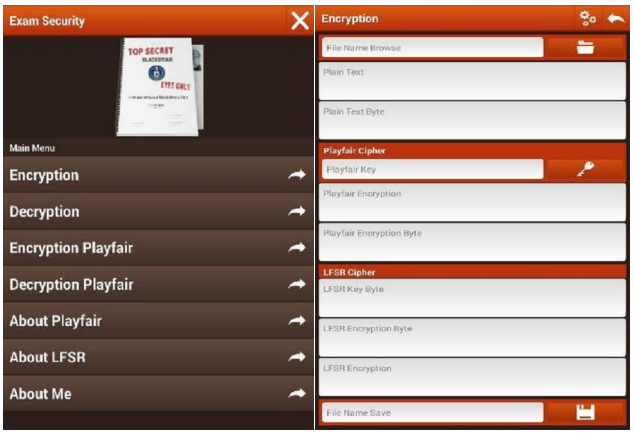
Gambar 5: Pembentukan Kunci LFSR

Pada tabel diatas memasukan inputan awal 10011001 maka output yang dihasilkan adalah 10011001 kemudian output berikutnya adalah 00010001 dan seterusnya sampai (n). Kemudian *Output* yang dihasilkan susun kedalam matriks berukuran (2 × n) dimana panjang (n) tersebut berdasarkan panjang dari baris yang terdapat pada *ciphertext*s yang telah dihasilkan dari proses enkripsi ke-1, yaitu menggunakan *playfair cipher.*

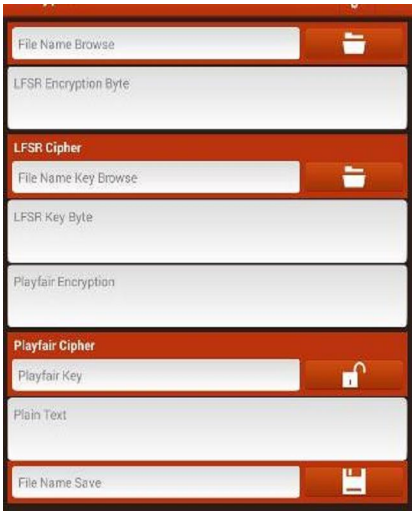
IV. HASIL DAN PEMBAHASAN

4.1. Konstruksi User Interface

User interface aplikasi yang dibangun dapat dilihat pada Gambar 6 dan Gambar 7:



Gambar 6: *Interface* Utama Aplikasi dan *Interface* Enkripsi



Gambar 7: *Interface* Deskripsi

4.2. Hasil Uji Keacakan Kriptografi Playfair Cipher Matriks 13x13 dan digabung dengan LFSR

Pada uji keacakan *ciphertexst* ini dilakukan sebanyak 30 kali percobaan dengan parameter sample yang berbeda-beda yaitu berdasarkan besar ukuran file,panjang karakter *ciphertext* dan kunci yang sama. Hasil yang didapat dari uji coba menggunakan aplikasi dilakukan perhitungan menggunakan metode *Avalanche Effect* dengan rumus :

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

Dimana jumlah perubahan *bit* didapat dari hasil perhitungan XOR antar *plaintext* dengan *ciphertext* yang terlebih dahulu dikonversi kedalam bilangan binner, lalu untuk membuktikan bahwa modifikasi algoritma *playfair* dengan matriks kunci 13x13 dan digabung dengan LFSR memiliki nilai keacakan *ciphertext* yang lebih tinggi, maka dilakukan perbandingan dengan metode sebelumnya. Berikut adalah hasil dari perbandingan uji keacakan *ciphertext* dapa dilihat pada Tabel 1 :

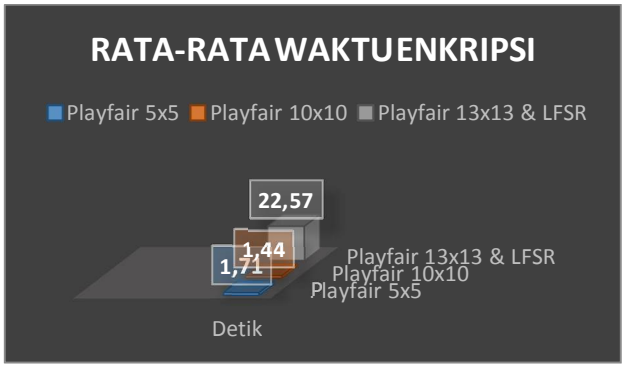
Tabel 1 : Perbandingan Hasil Uji Keacakan Ciphertext

No	Nama Data/File	Panjang Plaintext (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
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
Nilai Rata-Rata *Avalanche Efect*			**34,41**	**32,15**	**43,39**

4.3. Pengujian Kompleksitas Waktu

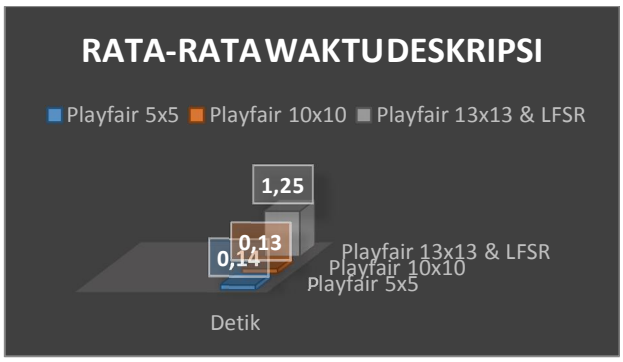
Pada pengujian kompleksitas waktu ini dilakukan sebanyak 30 kali percobaan dengan parameter sample yang berbeda-beda yaitu berdasarkan besar ukuran *file* dan panjang karakter *ciphertext*. Pengujian kompleksitas waktu ini didapat dari aplikasi saat melakukan proses enkripsi dan deskripsi. Setelah itu dilakukan perhitungan rata-rata waktu enkripsi dan deskripsi. Berikut adalah hasil dari uji kompleksitas waktu antara *Playfair* matriks kunci 13x3 dan digabung dengan LFSR, *Playfair* klasik martiks kunci 5x5 dan *Playfair* Matriks kunci 10x10 dapat dilihat pada Gambar 8, Gambar 9. Gambar 10 dan Gambar 11:

Gambar 8: Kompleksitas Waktu Enkripsi



Gambar 9: Rata-rata Waktu Enkripsi

Gambar 10: Kompleksitas Waktu Deskripsi



Gambar 11: Rata-rata Waktu Deskripsi

V. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, teknik kriptografi yang dibuat ini dapat menjawab hipotesis di awal penelitian yaitu modifikasi metode playfair dengan tabel 13 x 13 dan digabung dengan *linear feedback Shift Register* (LFSR) 8 bit, dapat memperbaiki kekurangan *playfair* sebelumnya seperti, dengan merubah ukuran matriks kunci 13x13 maka *playfair cipher* mampu menyisipkan karakter sebanyak 196 karakter terdiri dari huruf kapital, huruf kecil, angka dan beberapa simbol. Hasil perhitungan *avalanche effect* didapatkan nilai rata-rata dari algoritma *playfair cipher* yang dilakukan modifikasi kunci matriks 13x13 dan digabung dengan generator LFSR sebesar 43.59%, algoritma *playfair cipher* yang dilakukan modifikasi kunci matriks 10x10 tanpa digabung dengan LFSR sebesar 32.15% dan algoritma *playfair* klasik matriks 5x5 tanpa digabung dengan LFSR sebesar 34.41%.

Hal tersebut menunjukkan bahwa algoritma *playfair cipher* dengan matriks 13x13 dan digabung dengan generator LFSR memiliki *ciphertext* yang lebih acak dari *playfair cipher* sebelumnya dan dapat disimpulkan bahwa *playfair cipher* yang telah dimodifikasi dan digabung dengan generator LFSR ini lebih kuat dari *playfair cipher* sebelumnya, sehingga dapat lebih mempersulit kriptanalisis dalam menganalisa *bigram*. Hasil pengujian kompleksitas waktu dengan metode *Time Stamp Counter (TSC)* didapat waktu rata-rata enkripsi 22,57 detik pada metode *Playfair* 13x13 yang digabung dengan LFSR, 1,44 detik pada metode P*layfair* 10x10 dan 1,71 detik pada metode *Playfair* klasik 5x5, sedangkan nilai rata-rata waktu deskripsi 1,25 detik pada metode *Playfair* 13x13 yang digabung dengan LFSR, 1,13 detik pada metode P*layfair* 10x10 dan 1,14 detik pada metode *Playfair* klasik 5x5. Nilai pada metode *Playfair* 13x13 yang digabung dengan LFSR meskipun lebih besar dari metode *Playfair* 10x10 dan *Playfair* 5x5 akan tetapi ketiga metode tersebut tergolong memiliki waktu enkripsi dan dekripsi yang begitu cepat.

DAFTAR PUSTAKA

[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.