Buletin Sistem Informasi dan Teknologi Islam
Vol 3, No 1, Februari 2022, pp. 42-51
ISSN: 2721-0901

Implementasi Metode Kriptografi Menggunakan *Cipher* Subtitusi dan *Cipher* Transposisi pada Data Teks

Muhammad Alif Mubarak B[a,1,*], Yulita Salim[a,2], Sugiarti[a,3]

[a] *Universitas Muslim Indonesia, Jalan Urip Sumoharjo, Makassar, 90231*
[1] *mubarakalif526@gmail,com;* [2] *yulitasalim@umi.ac.id;* [3] *sugiarti.sugiarti@umi.ac.id;*
**corresponding author*

INFORMASI ARTIKEL

Diterima : 07 – 02 – 2022
Direvisi : 21 – 02 – 2022
Diterbitkan : 28 – 02 – 2022

Kata Kunci:
Kriptografi
Enkripsi
Dekripsi
Playfair Cipher
Zigzag Cipher

ABSTRAK

Masalah yang sering terjadi dalam komunikasi menggunakan jaringan internet seperti penyadapan, pencurian data, dan pengubahan data oleh pihak yang tidak berwenang. Hal ini menjadi alasan kenapa diperlukan keamanan data untuk mencegah atau mengurangi peluang terjadinya kejahatan terhadap informasi atau data yang bersifat rahasia. Tujuan dari penelitian kriptografi saat ini adalah bagaimana menerapkan metode kriptografi agar mendapatkan hasil enkripsi yang susah dipecahkan atau didekripsi oleh kripnatalis. Salah satu cara untuk melakukan proses enkripsi agar menghasilkan *cipher text* yang susah dipecahkan adalah konsep super enkripsi. Super enkripsi adalah proses enkripsi yang menggabungkan beberapa metode enkripsi atau melakukan proses enkripsi lebih dari satu kali untuk satu *plaintext*. Super enkripsi ini dapat diterapkan pada data yang bersifat rahasia dan penting karena tingkat optimalisasinya lebih tinggi. Hasil penelitian ini menunjukkan bahwa mengkombinasikan metode substitusi *cipher* dan transposisi *cipher* dapat dilakukan untuk melakukan proses kriptografi. Proses super enkripsi ini membutuhkan waktu lebih lama karena proses enkripsi dan dekripsi menggunakan dua metode, serta jumlah karakter *plaintext* yang dimasukkan juga ikut mempengaruhi waktu proses super enkripsi. Berdasarkan hasil pengujian yang dilakukan, untuk melakukan enkripsi dan dekripsi pada 3 *plaintext* yaitu *plaintext1*, *plaintext2*, *plaintext3* dengan menggunakan *key* sebanyak 20 karakter, membutuhkan waktu proses enkripsi yaitu *plaintext1* dengan jumlah karakter 19 selama 0.019 detik, *plaintext2* dengan jumlah karakter 86 selama 0.040 detik, dan *plaintext3* dengan jumlah karakter 158 selama 0.115 detik.

I. Pendahuluan

Perkembangan teknologi informasi menghasilkan banyak bentuk inovasi-inovasi digital yang sangat membantu kebutuhan manusia dengan berbagai keadaan. Selain itu, perkembangan teknologi juga menghasilkan banyak bentuk kejahatan-kejahatan salah satunya adalah kejahatan dalam aktivitas komunikasi yang dilakukan oleh pengguna internet. Bentuk komunikasi yang sering dilakukan dalam media komunikasi adalah komunikasi menggunakan teks. Komunikasi yang dilakukan oleh orang-orang terkadang membahas hal yang umum, penting, dan sampai pembahasan yang rahasia. Kejahatan-kejahatan dalam komunikasi menggunakan jaringan internet seperti penyadapan, pencurian data, dan pengubahan data oleh pihak yang tidak berwenang. Hal ini menjadi alasan kenapa diperlukan keamanan data untuk mencegah atau mengurangi peluang terjadinya kejahatan terhadap informasi atau data yang bersifat rahasia.

Kriptografi merupakan pembelajaran terhadap teknik matematis yang terkait dengan aspek keamanan [1] suatu sistem informasi, kerahasiaan (*privacy* atau *confidentiality*), integritas (*Integrity*), otentikasi (*Authentication*), dan pembuktian yang tak tersangkal (*Non-Repudation*) [2]. Kriptografi terdiri dari 2 aktivitas utama yaitu enkripsi dan dekripsi.

Enkripsi adalah kegiatan mengubah teks asli menjadi *cipher text*, sedangkan dekripsi adalah kegiatan mengubah *ciphertext* kembali menjadi teks asli [3]. Metode kriptografi secara umum dibedakan menjadi 2 jenis metode kriptografi yaitu metode substitusi dan metode transposisi. Kriptografi metode substitusi adalah metode kriptografi dengan memasukkan karakter-karakter *plaintext* kedalam tabel enkripsi sedangkam kriptografi metode transposisi adalah metode kriptografi dengan mengubah posisi dari karakter- karakter *plaintext* [4].

Penelitian-penelitian yang terkait dengan kriptografi sudah banyak dilakukan dengan menerapkan metode kriptografi sampai pada memodifikasi metode kriptografi. Penelitian yang dilakukan Dian Susanti dengan judul "Analisis Modifikasi Metode *Playfair Cipher* dalam Pengamanan Data Teks". Hasil penelitiannya adalah proses enkripsi menggunakan modifikasi metode *playfair cipher* dapat dilakukan dimana keamanan data teks menggunakan metode tersebut hanya ada layanan keamanan *Confidentiality* dan *Authentication* [5].

Tujuan dasar penelitian kriptografi adalah bagaimana menerapkan metode kriptografi agar mendapatkan hasil enkripsi yang susah dipecahkan atau dideskripsi oleh kripnatalis. Salah satu cara untuk melakukan proses enkripsi agar menghasilkan *cipher text* yang susah dipecahkan adalah konsep super enkripsi. Super enkripsi adalah proses enkripsi yang menggabungkan beberapa metode enkripsi atau melakukan proses enkripsi lebih dari satu kali untuk satu *plaintext* [4].

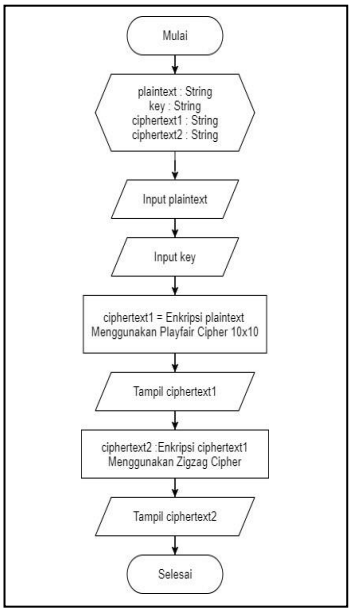
Super enkripsi ini dapat diterapkan pada data yang bersifat rahasia dan penting karena tingkat optimalisasinya lebih tinggi. Oleh karena itu, pada penelitian ini penulis akan menerapkan super enkripsi dalam mengamankan data teks dalam bentuk file berekstensi ".txt" dengan menggabungkan 2 metode enkripsi yang terdiri dari enkripsi substitusi dan enkripsi transposisi untuk mendapatkan hasil enkripsi yang susah dipecahkan oleh kripnatalis. Berdasarkan masalah yang diuraikan di atas, penulis mengangkat topik artikel yang berjudul "Implementasi Metode Kriptografi Menggunakan *Cipher* Subtitusi dan *Cipher* Transposisi pada Data Teks".

II. Metode

Pada perancangan proses enkripsi dan dekripsi ini menggunakan metode *Playfair Cipher* dan *Zigzag Cipher*. Adapun tahapannya adalah sebagai berikut.

A. Tahapan Proses Enkripsi

Pada perancangan proses enkripsi ini menggunakan metode Playfair Cipher 10×10 dan Zigzag Cipher sebanyak 100 karakter. Berikut adalah *flowchart* proses enkripsi yang dapat dilihat pada gambar 1.



Gambar 1. *Flowchart* Perancangan Proses Enkripsi

1) Pengimputan Plaintext dan Key Enkripsi

Proses enkripsi ini dimulai dari penginputan teks asli atau *plaintext* dan *key* untuk memproses enkripsi pada penginputan *plaintext* dan *key. Key* yang dimasukkan akan digunakan untuk enkripsi menggunakan *playfair cipher.*

2) Enkripsi Menggunakan Playfair Cipher

Proses enkripsi pada penelitian ini menggunakan *playfair cipher* 10×10. Proses enkripsi ini dilakukan dengan menginputkan *plaintext*. Dalam proses enkripsi ini, dibutuhkan sebuah key untuk proses enkripsi yang juga akan digunakan untuk proses deksripsi. Proses enkripsi dimulai setelah *user* menginputkan *plaintext* dan *key* enkripsi, *key* yang diinputkan diolah dengan menuliskan semua jenis karakter yang ada pada *key* kemudian selanjutnya digunakan untuk membentuk tabel *playfair cipher*. Pembentukan tabel *playfair cipher* 10×10 membutuhkan 100 karakter.

Pembentukan tabel *playfair cipher* ini dapat dilakukan apabila *key* enkripsi sudah siap. Proses ini dimulai dengan menyediakan tabel *playfair cipher* 10×10 yaitu 10 baris dan 10 kolom. Tabel ini akan dimulai dengan memasukkan karakter-karakter *key* enkripsi kemudian karakter-karakter selanjutnya secara terurut dan tidak menuliskan karakter key secara berulang dalam tabel.

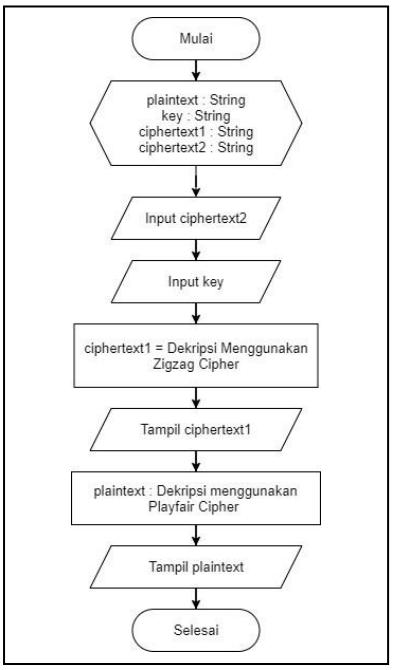
Proses enkripsi ini dilakukan dengan mengolah *plaintext* kedalam *bgram* yaitu membagi *plaintext* menjadi beberapa bagian yang terdiri dari 2 karakter. Setelah itu, masing-masing pasangan *bgram* akan dienkripsi menggunakan tabel dengan mencari letak masing-masing karakter di dalam tabel *playfair cipher*. Setelah setiap pasangan karakter (*bgram*) sudah diganti atau dienkripsi, maka semua pasangan karakter tersebut digabung dan membentuk *ciphertext* yang akan disebut sebagai *ciphertext playfair*.

3) Tahap Proses Dekripsi

Proses dekripsi adalah proses mengubah *ciphertext* menjadi *plaintext*. Proses dekripsi pada penelitian ini dilakukan dengan menggunakan dua metode yang sama dengan metode yang digunakan pada proses enkripsi. Pada proses dekripsi ini, *ciphertext* akan didekripsi menggunakan *Zigzag cipher* untuk mengubah *ciphertext* menjadi *ciphertext playfair*. Kemudian menggunakan metode *playfair cipher* untuk mengubah *ciphertext playfair* menjadi *plaintext* [6]. Berikut perancangan proses dekripsi dapat dilihat pada gambar *flowchart* berikut.

B. Tahapan Proses Dekripsi

Proses dekripsi adalah proses mengubah *ciphertext* menjadi *plaintext*. Proses dekripsi pada penelitian ini dilakukan dengan menggunakan dua metode yang sama dengan metode yang digunakan pada proses enkripsi [7]. Pada proses dekripsi ini, *ciphertext* akan didekripsi menggunakan *Zigzag cipher* untuk mengubah *ciphertext* menjadi *ciphertext playfair*. Kemudian menggunakan metode *playfair cipher* untuk mengubah *ciphertext playfair* menjadi *plaintext* [6]. Berikut perancangan proses dekripsi dapat dilihat pada gambar *flowchart* berikut.



Gambar 2. *Flowchart Perancangan Dekripsi*

1) Pengimputan Ciphertext dan Key

Proses dekripsi ini dimulai dari penginputan teks asli atau *ciphertext* dan *Key* untuk memproses enkripsi. Pada penginputan *ciphertext* dan *key*. *Ciphertext* merupakan hasil enkripsi dari sistem enkripsi yang dibuat, dan key meruakan *key* yang sama dengan *key* untuk proses enkripsi.

2) Deskripsi menggunakan Zigzang Capher

Ciphertext yang diinputkan oleh *user* yang akan di dekripsi merupakan hasil enkripsi menggunakan dua metode enkripsi. Untuk melakukan proses dekripsi, maka *ciphertext* akan didekripsi dengan menggunakan metode *zigzag cipher* terlebih dahulu untuk mendapatkan *ciphertext playfair*.

Untuk proses dekripsi, jumlah karakter yang akan didekripsi harus diketahui. Setelah itu membuat 3 baris dengan masing-masing baris terdiri dari kolom yang jumlahnya sama dengan jumlah karakter teks yang akan didekripsi. Kemudian memasukka *ciphertext* ke setiap baris. Pada baris pertama, karakter

diinputkan mulai dari kolom index 0 dengan masing-masing karakter berada pada jarak 2 index. Pada baris kedua, karakter diinputkan mulai dari kolom index 1 dengan masing- masing karakter berada pada jarak 1 index. Dan pada baris ketiga, karakter diinputkan mulai dari kolom index 2 dengan masing-masing karakter berada para jarak 2 index. Setelah setiap karakter pada teks yang didekripsi selesai, selanjutnya adalah mengambil karakter berupabaris i kolom j, selanjutnya baris i+1 kolom j+1, selanjutnya baris i+2 kolom j+2, dan baris i+1 kolom j+3. Setelah itu maka didapatkan hasil dekripsi menggunakan *zigzag cipher*. Pada penelitian ini hasil dekripsi menggunakan metode *zigzag cipher* disebut dengan *ciphertext playfair*

3) Deskripsi Menggunakan Playfair Cipher

Ciphertext playfair adalah hasil dekripsi menggunakan metode *zigzag cipher* dari *ciphertext*. Selanjutnya adalah mengubah *ciphertext playfair* menjadi *plaintext*. Proses dekripsi pada penelitian ini,membutuhkan sebuah teks untuk didekripsi yang merupakan hasil dari dekripsi menggunakan *zigzag cipher* dan *key* diambil dari inputan *user* pada saat akan melakukan dekripsi.

III.Hasil dan Pembahasan

A. Implementasi Antarmuka

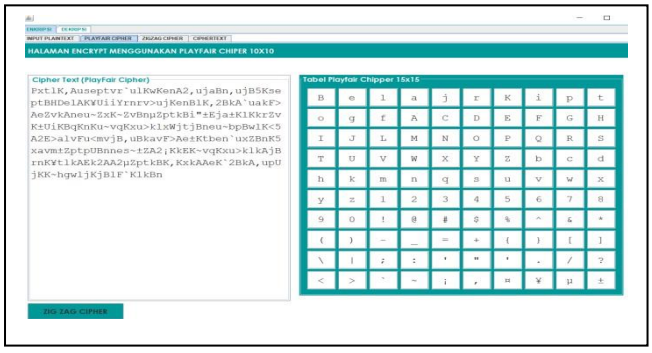
1) Antarmuka Proses Enkripsi

Implementasi Antarmuka untuk proses enkripsi terdiri dari beberapa halaman untuk menggambarkan tahapan-tahapan super enkripsi yang dilakukan.

a) Implementasi Halaman Input Plaintext

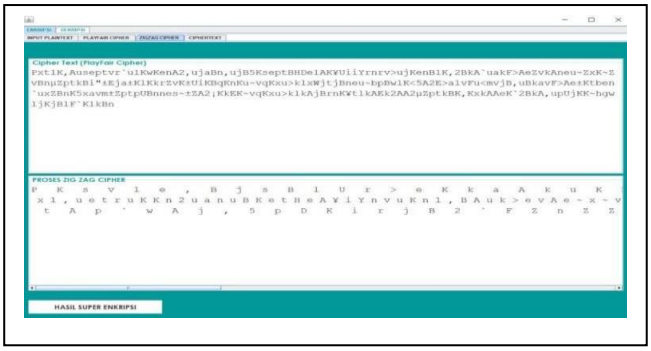
Gambar 3. Implementasi Halaman Input *Plaintext*

b) Implementasi Halaman Enkripsi Playfair Cipher



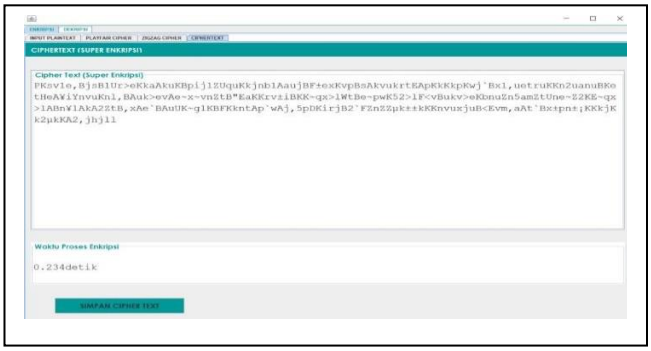
Gambar 4. Implementasi Halaman Enkripsi *Playfair Cipher*

c) Implementasi Halaman Enkripsi Zigzag Cipher



Gambar 5. *Implementasi Halaman Enkripsi Zigzag Cipher*

d) Implementasi Halaman Hasil Enkripsi



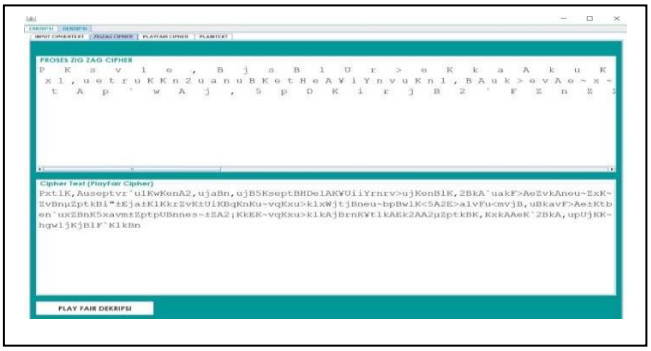
Gambar 6. Implementasi Halaman Hasil Enkripsi

2) Antarmuka Proses Dekripsi

a) Implementasi Halaman Input Ciphertext

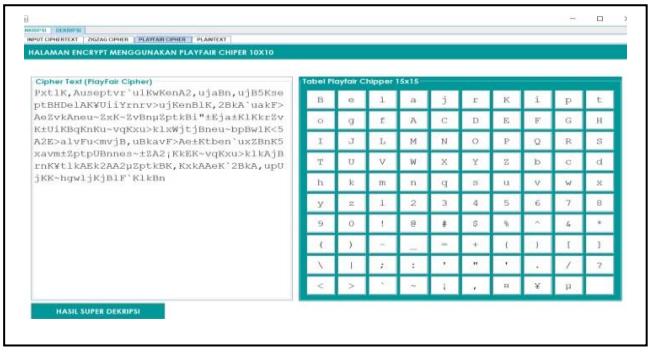
Gambar 7. Implementasi Halaman *Input Ciphertext*

b) Implementasi Halaman Dekripsi Zigzag Cipher



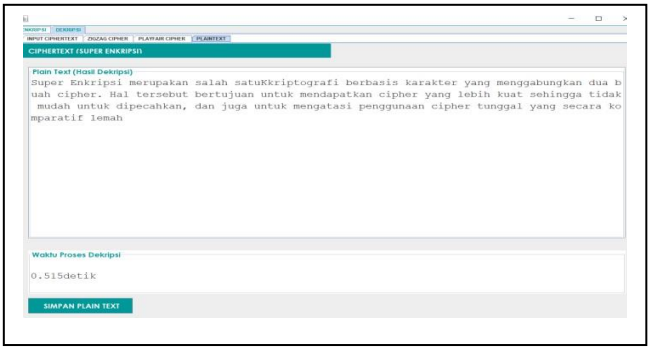
Gambar 8. Iplementasi Halaman Dekripsi *Zigzag Cipher*

c) Implementasi Halaman Dekripsi Playfair Cipher



Gambar 9. Implementasi Halaman Dekripsi *Playfair Cipher*

d) Implementasi Halaman Hasil Dekripsi



Gambar 10. Implementasi Halaman Hasill Dekripsi

B. Pembahasan Implemenntasi Enkripsi dan Dekripsi

1) Proses Enkripsi Playfair Cipher

a) Proses Enkripsi Playfair Cipher

Pada penelitian ini, proses enkripsi tahap pertama adalah enkripsi menggunakan *playfair cipher*. Berikut *plaintext* yang akan dienkripsi adalah sebagai berikut.

Plaintext : Fakultas Ilmu Komputer
Key : Makassar, 6/21/2021

- Mengolah Key dengan menghilangkan karakter yang sama. Key yang diinputkan adalah "Makassar, 6/21/2021", maka hasil pengolahan key dapat dilihat berikut ini.
  Key : Makassar, 6/21/2021
  Hasil Key : 'M', 'a', 'k', 's', 'r', ',', '6', '/', '2', '1', '0'
- Pembentukan tabel *playfair cipher* yang terbentuk dari karakter-karakter yang ada dalam *database* dimana dalam mengisi tabel enkripsi dimulai dengan karakter-karakter yang membentuk *key* enrkipsi diikuti oleh karakter lainnya.

M	a	k	s	r	,	6	/	2	1
0	A	B	C	D	E	F	G	H	I
J	K	L	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	b	c	d	e
f	g	h	i	j	l	m	n	o	p
q	t	u	v	w	x	y	z	3	4
5	7	8	9	!	@	#	$	%	^
&	*	(	)	-	_	=	+	{	}
[	]	\	|	;	:	'	"	'	.
?	<	>	`	~	¡	¤	¥	µ	±

Gambar 11. Tabel *Playfair Cipher* Enkripsi

- *Plaintext* yang sudah diinputkan selanjutnya akan diubah kedalam bentuk *bi-gram* yaitu memisahkan masing-masing 2 karakter. Berikut hasil proses pembentukan *bi-gram* dari *plaintext* yang diinputkan.
  Plaintext :
  Fakultas Ilmu Komputer
  Bi-gram Plaintext :
  Fa ku lt as Il mu Ko mp ut er
- Setelah itu, maka proses enkripsi dilakukan dengan memerhatikan aturan umum dari proses enkripsi. Hasil dari proses enkripsi adalah cipher text yaitu sebagai berikut. ***Ciphertext*** : A6B8gxkrEphySgnqvtY1

b) Proses Enkripsi Zigzag Cipher

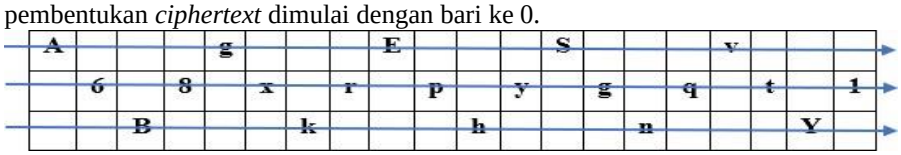
Proses enkripsi *zigzag cipher* dilakukan setelah plaintext telah dienkripsi menggunakan *playfair cipher*. Proses enkripsi menggunakan *zigzag cipher* dilakukan terhadap hasil enkripsi dari *playfair cipher* yang selanjutnya disebut sebagai *ciphertext1*.

Ciphertext1 : Fakultas Ilmu Komputer
Kunci : 3
Offset : 0

- Menghitunng panjang karakter dari *ciphertext1* (teks yang akan dienkripsi).
  Ciphertext1 : A6B8gxkrEphySgnqvtY1
  Panjang Karakter : 20 karakter
- Membuat tabel dengan jumlah baris 3 karena key untuk *zigzag cipher* itu 3, dan 20 kolom karena jumlah karakter 20.
- Mengisi Tabel yang telah dibuat dengan karakter teks yang akandienkripsi membentuk model *zigzag*.

A				g				E				S				v			
	6		8		x		r		p		y		g		q		t		1
		B				k				h				n				Y	

- Membentuk *ciphertext* (hasil enkripsi) dengan menggabungkankarakter pada tabel. Karena pada penelitian ini, ditentukan *zigzag* dengan *offset* sama dengan 0, maka pembentukan *ciphertext* dimulai dengan bari ke 0.



Sehingga *ciphertext* yang terbentuk adalah **AgESv68xrpygqt1BkhnY**.

2) Pembahasan Implementasi Dekripsi

a) Proses Dekripsi Zigzag Cipher

Proses dekripsi menggunakan *zigzag cipher* adalah proses dekripsi dengan mengubah *plaintext* menjadi teks yang asli. Pada penelitian ini, proses dekripsi dilakukan dengan menggunakan metode *zigzag cipher* untuk mengubah *ciphertext* menjadi *ciphertext1*. Berikut *ciphertext* yang akan diubah menjadi *ciphertext1*.

Ciphertext1 : AgESv68xrpygqt1BkhnY
Key : 3
Offset : 0

- Menghitunng panjang karakter dari *ciphertext1* (teks yang akandidekripsi).
  Ciphertext1 : AgESv68xrpygqt1BkhnY
  Panjang Karakter : 20 karakter
- Membuat tabel dengan jumlah baris 3 karena *key* untuk *zigzag cipher* itu 3, dan 20 kolom karena jumlah karakter 20.
- Mengisi Tabel yang telah dibuat dengan karakter teks yang akan dienkripsi membentuk model *zigzag*

A				g				E				S				v			
	6		8		x		r		p		y		g		q		t		1
		B				k				h				n				Y	

- Membentuk *ciphertext* (hasil dekripsi) dengan menggabungkankarakter pada tabel dengan cara *zigzag*. Berikut hasil dekripsi dari proses tersebut adalah A6B8gxkrEphySgnqvtY1.

b) Proses Enkripsi Playfair Cipher

Pada penelitian ini, proses dekripsi tahap kedua adalah dekripsimenggunakan *playfair* ***cipher***. Berikut *plaintext* yang akan dienkripsi adalah sebagai berikut.

Plaintext : A6B8gxkrEphySgnqvtY1
Key : Makassar, 6/21/2021

- Mengolah *Key* dengan menghilangkan karakter yang sama. *Key* yang diinputkan adalah "Makassar, 6/21/2021", maka hasil pengolahan *key* dapat dilihat berikut ini.
  Key : Makassar, 6/21/2021
  Hasil Key : 'M', 'a', 'k', 's', 'r', ',', '6', '/', '2', '1', '0'

- Pembentukan tabel *playfair cipher* yang terbentuk dari karakter-karakter yang ada dalam *database* dimana dalam mengisi tabel enkripsi dimulai dengan karakter-karakter yang membentuk key enrkipsi diikuti oleh karakter lainnya.

Gambar 12. Tabel *PlayFair Cipher* Enkripsi

- *Plaintext* yang sudah diinputkan selanjutnya akan diubah kedalam bentuk *bi-gram* yaitu memisahkan masing-masing 2 karakter. Berikut hasil proses pembentukan *bi-gram* dari *plaintext* yang diinputkan.

  Plaintext : A6B8gxkrEphySgnqvtY1

  Bi-gram Plaintext : A6 B8 gx kr Ep hy Sg nq vt Y1

- Setelah itu, maka proses enkripsi dilakukan dengan memerhatikan aturan umum dari proses enkripsi. Berikut hasil enkripsi dari *plaintext* yang telah dilakukan.

  Ciphertext : Fakultas Ilmu Komputer

C. Pengujian Sistem

Uji coba sistem adalah tahapan pengujian terhadap kecepatan proses enkripsi dan dekripsi menggunakan 3 jenis plaintext dan 3 jenis key untuk melihat kecepatan proses enkripsi dan dekripsi dilihat dari Panjang *plaintext*/*ciphertext* dan Panjang *key*.

M	a	k	s	r	,	6	/	2	1
0	A	B	C	D	E	F	G	H	I
J	K	L	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	b	c	d	e
f	g	h	i	j	l	m	n	o	p
q	t	u	v	w	x	y	z	3	4
5	7	8	9	!	@	#	$	%	^
&	*	(	)	-	_	=	+	[	]
[	]	\	|	;	:	'	"	'	.
?	<	>	`	~	¡	¤	¥	µ	±

Gambar 12. Tabel *Playfair Cipher* Enkripsi

Tabel 1. *Plaintext* Uji Coba

No	*Plaintext*	Jumlah Karakter
1	Metode *zig-zag cipher*	19
2	Metode *zig-zag cipher* merupakan salah satu algoritma kriptografi klasik dengan teknik transposisi.	86
3	Metode zig-zag cipher merupakan salah satu algoritma kriptografi klasik dengan teknik transposisi yang juga merupakan pembentukan dari algoritma transposisi kolom (*Columnar Transposition Cipher*) dan transposisi Rail *Fance Cipher* [8].	221

Tabel 2. *Key* Uji Coba

No	*Key*	Jumlah Karakter
1	*Chips*	5 Karakter
2	Barru, 2021	10 Karakter
3	Makassar, 24 Juni 2021.	20 Karakter

D. Hasil Pengujian

Hasil dari proses pengujian yang akan dilakukan adalah membandingkan durasi enkripsi dan dekripsi 3 *plaintext* terhadap 3 *key*. Adapun hasil dari pengujian yang dilakukan adalah sebagai berikut.

Tabel 3. Pengujian Durasi Enkripsi

Plain Text / *Key*	*Plaintext* 1	*Plaintext* 2	*Plaintext* 3
*Key*1	0.029detik 0.016detik 0.009detik Rata-rata: 0.018	0.37detik 0.37 detik 0.046 detik Rata-rata: 0.040	0.140 detik 0.110 detik 0.107 detik Rata-Rata: 0.119
*Key*2	0.015detik 0.016detik 0.011 detik Rata-rata: 0.014	0.048 detik 0.050 detik 0.045 detik Rata-rata: 0.048	0.109 detik 0.112 detik 0.120 detik Rata-rata: 0.114
*Key*3	0.019detik 0.017detik 0.022detik Rata-rata: 0.019	0.042 detik 0.040 detik 0.039 detik Rata-rata: 0.040	0.113 detik 0.106 detik 0.126 detik Rata-rata: 0.115

Tabel 4. Pengujian Durasi Dekripsi

Plain Text / *Key*	*Plaintext* 1	*Plaintext* 2	*Plaintext* 3
*Key*1	0.019 detik 0.010 detik 0.013 detik Rata-rata : 0.014	0.031 detik 0.028 detik 0.036 detik Rata-rata: 0.032	0.130 detik 0.107 detik 0.114 detik Rata-Rata:0.117
*Key*2	0.016 detik 0.017 detik 0.013 detik Rata-rata :0.015	0.050 detik 0.045 detik 0.048 detik Rata-rata :0.048	0.120 detik 0.114 detik 0.120 detik Rata-rata :0.118
*Key*3	0.020 detik 0.017 detik 0.018 detik Rata-rata :0.018	0.044 detik 0.040 detik 0.038 detik Rata-rata : 0.041	0.120 detik 0.123 detik 0.134 detik Rata-rata :0.126

Proses pengujian dari proses enkripsi dan dekripsi yang telah dilakukan terhadap 3 jenis *plaintext* dan 3 jenis *key*, dapat dilihat dari hasil percobaan bahwa lambat cepatnya proses enkripsi dan dekripsi itu dipengaruhi oleh panjang *plaintext / ciphertext* yang diinputkan, dimana semakin panjang *plaintext / ciphertext* yang digunakan maka semakin lama waktu yang dibutuhkan untuk proses enkripsi dan dekripsi. Panjang *key* dalam proses enkripsi / dekripsi tetap berpengaruh dengan waktu proses enkripsi / dekripsi tetapi tidak menghasilkan rentang waktu yang jauh berbeda.

IV. Kesimpulan dan saran

Berdasarkan pembahasan pada bab-bab sebelumnya maka penulis dapat mengambil kesimpulan super enkripsi dengan mengkombinasikan metode substitusi *cipher* dengan transposisi cipher dapat dilakukan untuk melakukan penyandian teks, waktu yang dibutuhkan dalam melakukan proses super enkripsi dengan mengkombinasikan dua metode membutuhkan waktu yang lebih lama karena proses enkripsi maupun dekripsi dilakukan sebanyak 2 kali dibandingkan dengan menggunakan satu metode, durasi untuk melakukan enkripsi dan dekripsi dipengaruhi oleh Panjang *plaintext* / *ciphertext* yang diinputkan. Semakin Panjang *plaintext* / *ciphertext* yang diinputkan maka membutuhkan waktu lebih lama untuk melakukan proses enkripsi dan dekripsi. Beberapa saran yang mungkin dapat digunakan dalam pengembangan sistem ini kedepannya pada penelitian ini metode *zigzag cipher* masih menggunakan *key* dan *offset* yang statik sehingga selanjutnya dapat melakukan enkripsi dan dekripsi yang bersifat lebih dinamis. Penelitian selanjutnya, bisa mengimplementasikan proses super enkripsi dalam melakukan pengamanan file seperti gambar atau audio.

Daftar Pustaka

[1] A. R. Tuasikal, D. Indra, and F. Fattah, "Analisis Perbandingan Known Plaintext dan Chosen Plaintext Pada Metode Hill Chiper," *Bul. Sist. Inf. dan Teknol. Islam*, vol. 1, no. 1, pp. 1–4, 2020.

[2] D. P. O. Simamora, "Implementasi Algoritma RC4 dan Playfair Cipher untuk Menggunakan Data Teks," *J. Pelita Inform.*, vol. 16, pp. 328–334, 2017.

[3] R. K. Hondro, "Aplikasi Enkripsi Dan Dekripsi Sms Dengan Algoritma," no. July 2015, 2015.

[4] E. Setyaningsih, C. Iswahyudi, and N. Widyastuti, "Konsep Super Enkripsi untuk Meningkatkan Keamanan Data Citra," *Pros. Semin. Nas. Sist. Teknol. Inf. (SNASTI) 2011*, p. ISLP 7-ISLP 10, 2011.

[5] D. Susanti, "Analisis Modifikasi Metode Playfair Cipher Dalam Pengamanan Data Teks," *Indones. J. Data Sci.*, vol. 1, no. 1, pp. 11–18, 2020, doi: 10.33096/ijodas.v1i1.4.

[6] P. Rahardika, "Program Studi Informatika Fakultas Teknologi Informasi Dan Elektro Universitas Teknologi Yogyakarta 2020," 2020.

[7] Y. Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 29–37, 2019.

[8] A. Hariati, K. Hardiyanti, and W. E. Putri, "Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks," *Sinkron*, vol. 2, no. 2, pp. 13–17, 2018.