Indonesian Journal of Data and Science ISSN: 2715-9930
Vol 1, No 1, Maret 2020, pp. 11-18

Analisis Modifikasi Metode Playfair Cipher Dalam Pengamanan Data Teks

Dian Susanti[a,1]

[a] *Universitas Muslim Indonesia, Jln. UripSumoharjo Km.5 , Makassar 90231, Indonesia*
[1] *dian.susanti.fikom@gmail.com*

INFORMASI ARTIKEL

Diterima : 10 Januari 2020
Direvisi : 30 Februari 2020
Diterbitkan : 31 Maret 2020

Kata Kunci:
Playfair Cipher
Confidentiality
Authentication
Kunci simetris
plaintext

ABSTRAK

Dunia berkembang kian cepat seiring majunya teknologi informasi. Komunikasi kini menjadi tidak terbatas. Dengan banyaknya kemudahan untuk melakukan pengaksesan informasi, adakalanya diperlukan pengamanan informasi tersebut. Pengamanan ini berfungsi menangani pencegahan atas sampainya informasi ke tangan yang tidak berhak yang dapat menimbulkan kerugian bagi pemilik informasi. Metode Playfair Cipher merupakan salah satu metode yang digolongkan dalam kriptografi klasik yang proses enkripsinya menggunakan pemrosesan dalam bentuk blok-blok yang sangat besar. Metode Playfair Cipher menggunakan pembentukan tabel berdasarkan kunci yang diketahui. Penulis melakukan modifikasi metode Playfair Cipher menggunakan tabel 8x8 ini mempersulit pemecahan analisis digram dan frekuensi analisis karena semakin acak isi tabel akan menghasilkan ciphertext yang acak. Hasil pengujian ini yaitu pada aplikasi ini memberi dua layanan keamanan data saja yaitu Confidentiality dan Authentication, penggunaan kunci Metode Playfair Cipher jika penggunaan kunci yang digunakan panjangnya lebih pendek maka semakin cepat juga waktu enkripsi dan dekripsinya dan terdapat karakter tambahan yaitu karakter Space.

(cc) BY-NC

I. Pendahuluan

Dunia berkembang kian cepat seiring majunya teknologi informasi. Komunikasi kini menjadi tidak terbatas. Dengan banyaknya kemudahan untuk melakukan pengaksesan informasi, adakalanya diperlukan pengamanan informasi tersebut[1]. Pengamanan ini berfungsi menangani pencegahan atas sampainya informasi ke tangan yang tidak berhak yang dapat menimbulkan kerugian bagi pemilik informasi[2].

Kriptografi merupakan ilmu sekaligus seni untuk menjaga kerahasiaan data atau informasi dengan cara menyamarkannyamenjadi bentuk tersandi yang tidak bermakna. Metode kriptografi tersebut banyak digunakan untuk pengamanan data atau informasi saat ini. Peran kunci yang digunakan pada metode kriptografi adalah suatu informasi yang mengendalikan jalannya sebuah metode kriptografi[3].

Metode Playfair Cipher merupakan salah satu metode yang digolongkan dalam kriptografi klasik yang proses enkripsinya menggunakan pemrosesan dalam bentuk blok-blok yang sangat besar. Metode Playfair Cipher menggunakan pembentukan tabel berdasarkan kunci yang diketahui.

Komponen yang penting pada metode playfair adalah tabel cipher yang digunakan untuk melakukan enkripsi dan dekripsi tabel bawaan yang diperkenalkan oleh playfair adalah tabel yang berbentuk matrik berukuran (5x5) yang berisi huruf kapital dari A-Z dengan menghilangkan J. Tabel bawaan yang ada pada Playfair Cipher tidak dapat mengenkripsi Plaintext yang berisi angka (0-9) dan simbol-simbol Nurkifli (2014).

Kelemahan yang lain pada playfair adalah terjadinya ambigu pada hasil dekripsi karena pada persiapan enkripsi, Playfair Cipher memiliki mekanisme mengganti J dengan I dan jumlah karakter pada tabel 5x5 itu terbatas. Untuk memperkuat kerahasian data yang menggunakan metode ini, maka akan dilakukan penelitian dengandasar dari tabel playfair cipher dengan berbentuk tabel berukuran (8x8) yang pernah diteliti oleh Shivastava dkk (2011) dan Tunga dkk (2014) lalu di modifikasi dengan mengganti urutan tabel mengikuti tabel ASCII dan mengganti dua karakter yang digunakan Shivastava dkk (2011) yang dapat digunakan untuk melakukan enkripsi huruf, angka dan simbol.

Karena itu muncul suatu gagasan yang mengacu pada hal tersebut, yaitu untuk menganalisis layanan keamanan serta penggunaan kunci rahasia yang digunakan oleh metode Playfair Cipher.

Penelitian ini penulis mencoba membahas mengenai pengamanan data atau informasi dengan judul "Analisis Modifikasi Metode Playfair Dalam Pengamanan Data Teks".

II. Metode

A. Kriptografi

Bagian ini membahas konsep-konsep dasar dan istilah-istilah yang digunakan dalam kriptografi. Menuru Munir (2006) Kriptografi merupakan ilmu sekaligus seni untuk menjaga kerhasiaan data atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak bermakna. Metode kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. Kriptografi ini melakukan pengacakan huruf pada kata terang atau plaintext. Kriptografi ini hanya melakukan pengacakan pada huruf A – Z, dan sangatlah tidak disarankan untuk mengamankan informasi-informasi penting karena dapat dipecahkan dalam waktu singkat. Biarpun telah ditinggalkan, kriptografi klasik tetap dapat ditemui disetiap pelajaran kriptografi sebagai pengantar kriptografi modern. Kriptogarfi klasik memiliki beberapa ciri yaitu, berbasis karakter, menggunakan pena dan kertas saja saat belum ada komputer, termasuk ke dalam kriptografi kunci simetris[4].

Metode kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Pada kriptografi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Algoritma kriptografi modern umumnya beroperasi dalam mode bit. Berbeda dengan kriptografi klasik yang beroperasi dalam mode karakter (seperti yang dilakukan pada cipher substitusi atau cipher transposisi dari algoritma kriptografi klasik). Operasi dalam mode bit berarti semua data dan informasi (baik kunci, plainteks, maupun cipherteks) dinyatakan dalam rangkaian (string) bit biner, 0 dan 1. Algoritma enkripsi dan dekripsi memproses semua data dan informasi dalam bentuk rangkaian bit. Rangkaian bit yang menyatakan plainteks di enkripsi menjadi cipherteks dalam bentuk rangkaian bit, demikian sebaliknya [5].

Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah data atau informasi (yang disebut plaintext) menjadi pesan yang tersembunyi (disebut ciphertext). Metode dari enkripsi adalah fungsi yang digunakan untuk melakukan fungsi enkripsi dan dekripsi. Metode yang digunakan menentukan kekuatan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika.

Menurut Sadikin (2012), kriptografi mempunyai beberapa layanan keamanan antara lain sebagai berikut:

1. Confidentiality (kerahasaian)

   yaitu aspek yang berhubungan dengan penjagaan isi informasi dari siapapun kecuali yang mempunyai kewenangan atau kunci rahasia untuk membuka informasi.
2. Data Integrity (keutuhan data)

   adalah memastikan bahwa yang diterima oleh penerima adalah benar-benar sama dengan data yang dikirim oleh pengirim.
3. Authentication (otentikasi)

   yaitu aspek yang berhubungan dengan identifikasi atau pengenalan baik secara kesatuan sistem maupun informasi itu sendiri.
4. Non repudiation (menolak penyangkalan)

   merupakan usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman suatu informasi oleh yang mengirimkan.

Metode kriptografi adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan deskripsi. Metode kriptografi terbagi menjadi dua bagian yaitu metode simetris dan algortima asimetris. Metode simetris adalah metode yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya[6].

Dalam hal ini digunakan metode simestris dimana pengirim dan penerima harus menyepakati kunci yang akan dipakai dalam proses komunikasi. Membocorkan kunci kepada orang yang tidak berhak menyebabkan hilangnya kerahasiaan pesan. Jadi keamanan metode ini tergantung pada kuncinya [7].

Metode ini disebut juga sebagai algortima kunci rahasia atau metode satu kunci yaitu metode simetris. Metode asimetris yang disebut juga sebagai metode kunci publik. Kunci publik digunakan untuk mengenkripsi data atau informasi sedangkan kunci rahasia digunakan untuk mendeskripsi data atau informasi.

B. Playfair Cipher

Metode Playfair Cipher merupakan salah satu metode yang digolongkan dalam kriptografi klasik yang proses enkripsinya menggunakan pemrosesan dalam bentuk blok-blok yang sangat besar (Putri, dkk, 2018). Metode Playfair termasuk ke dalam polygram cipher (salah satu tipe dari cipher substitusi). Ditemukan oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada tanggal 26 Maret 1854. Playfair Cipher digunakan oleh tentara Inggris pada Perang Boer (Perang Dunia I).

Playfair Cipher merupakan metoda enkripsi klasik yang sangat sulit untuk dikriptanalisis secara manual. Meskipun demikian playfair dapat dipecahkan dengan menggunakan informasi frekuensi kemunculan bigram. Komponen yang penting pada metode playfair adalah tabel cipher yang digunakan untuk melakukan enkripsi dan dekripsi tabel bawaan yang diperkenalkan oleh playfair adalah tabel yang berbentuk matrik berukuran (5x5) yang berisi huruf kapital dari A- Z dengan menghilangkan huruf J digantikan dengan huruf I.

Berikut adalah beberapa aturan dari metode Playfair Cipher yaitu sebagai berikut:

1. Apabila terdapat huruf J, maka digantikan dengan huruf I.
2. Tulis pesan dalam pasangan huruf yaitu pisahkan dua-dua huruf.
3. Tidak boleh terdapat huruf yang sama, maka sisipkan huruf atau karakter yang jarang digunakan di tengahnya.
4. Apabila terdapat jumlah huruf ganjil, maka tambahkan huruf atau karakter yang jarang digunakan di akhir dari tabel yang telah dibentuk.

Playfair merupakan digraphs cipher, artinya setiap proses enkripsi dilakukan pada setiap dua huruf. Misalkan plaintext "KRIPTOLOGI", maka menjadi "KR|IP|TO|LO|GI". Kunci yang digunakan berupa kata dan tidak ada huruf sama yang berulang. Apabila kuncinya "SARAPAN", maka kunci yang digunakan adalah "SARPN". Selanjutnya, kunci dimasukkan ke dalam tabel, isian pertama adalah kunci, selanjutnya tulis huruf-huruf berikutnya secara urut dari baris pertama dahulu, bila huruf telah muncul, maka tidak dituliskan kembali. Gambar 1. Menunjukkan contoh penggunaan kunci pada tabel 5x5.

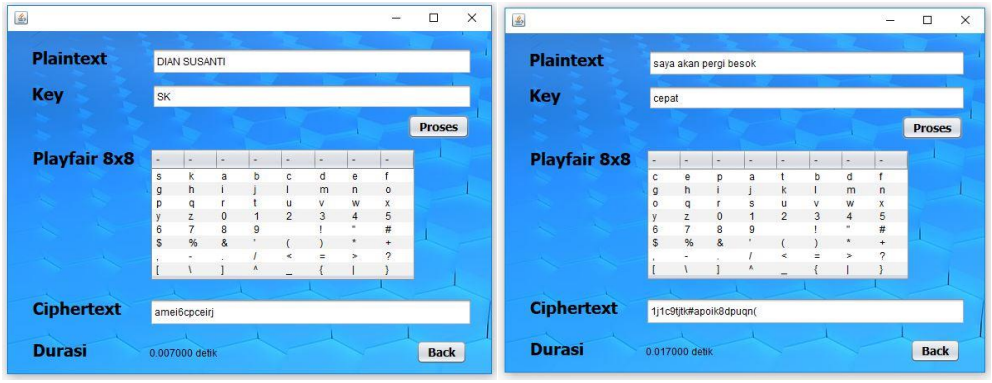
S	A	R	P	N
B	C	D	E	F
G	H	I	K	L
M	O	Q	T	U
V	W	X	Y	Z

Gambar 1. Penggunaan kunci Sarapan pada tabel 5x5

III. Hasil dan Pembahasan

A. Implementasi manual program

Responding huruf besar/huruf kecil dimana telah diatur penginputan huruf kapital menjadi huruf kecil. Seperti Gambar 4.8.



(a)huruf kapital (b)huruf non kapital

Gambar 2. Penginputan huruf kapital dan non kapital

Perhitungan manual dengan hasil perhitungan aplikasi, untuk membandingkan apakah asilnya benar-benar sama yang dihasilkan dari perhitungan aplikasi. Adapun perhitungan manualnya yaitu sebagai berikut :

Penyelesainnya Enkripsinya:

Plainteks : menggunakannya

Key : dian

Pisahkan perdua karakter atau huruf plainteksnya dimana jika huruf ganjil ditambahkan karakter + dan jika huruf sama maka sisipkan karakter +.

Plainteks : menggunakannya

: me ng gu na ka n+ ny a+

Selanjutnya periksa kunci sebelum memasukkan ke tabel 8x8 dengan tidak memasukkan huruf yang sudah ada maka huruf kunci yang dimasukkan yaitu :

Key : dian = **dian**

Kunci/key yang dimasukkan yaitu **dian**

Kunci dian

d	i	a	n	b	c	e	f
g	h	j	k	l	m	o	p
q	r	s	t	u	v	w	x
y	z	0	1	2	3	4	5
6	7	8	9	Spc	!	“	#
$	%	&	‘	(	)	*	+
,	-	.	/	<	=	>	?
[	\	]	^	_	{	|	}

Setelah kunci dimasukkan pada tabel maka sekarang mengekripsi plainteks yang sudah dipisahkan menjadi dua-dua karakter/huruf dengan mengikuti algoritma enkripsi *Playfair Cipher* sebagai berikut :

me : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **me = oc**.

ng : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **ng = dk**.

gu : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **gu = lq**.

na : beda kolom sama baris, maka ambil huruf/karakternya disebalahkannya masing-masing huruf/karakter. Jadi **na=bn**.

ka : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **ka = jn**.

n+ : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **n+ = f”**.

ny : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **ny = dl**.

a+ : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **a+ = f&**.

Jadi, me ng gun a ka n+ ny a+ = ocdklqbnjnf”dlf&.

Hasilnya yaitu cipherteks = **ocdklqbnjnf”dlf&**.

Penyelesainnya Dekripsinya:

Cipherteks : ocdklqbnjnf”dlf&

Key : dian

Pisahkan perdua karakter/huruf cipherteksnya.

Plainteks : ocdklqbnjnf'dlf&

: oc dk lq bn jn f' dl f&

Selanjutnya periksa kunci sebelum memasukkan ke tabel 8x8 dengan tidak memasukkan huruf yang sudah ada maka huruf kunci yang dimasukkan yaitu :

Key : dian = **dian**

Kunci/key yang dimasukkan tabelnya dapat di lihat pada Tabel 4.1 Kunci Dian.

Setelah kunci dimasukkan pada tabel maka sekarang mengdekripsi *cipher* teks yang sudah dipisahkan menjadi dua-dua karakter/huruf dengan kebalikan dari algoritma enkripsi *Playfair Cipher* sebagai berikut :

oc : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **oc=me**.

dk : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **dk=ng**.

lq : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **lq=gu**.

bn : beda kolom sama baris, maka ambil huruf/karakternya disebalahkannya masing-masing huruf/karakter. Jadi **bn=na**.

jn : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **jn=ka**.

f' : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **f'=n+**.

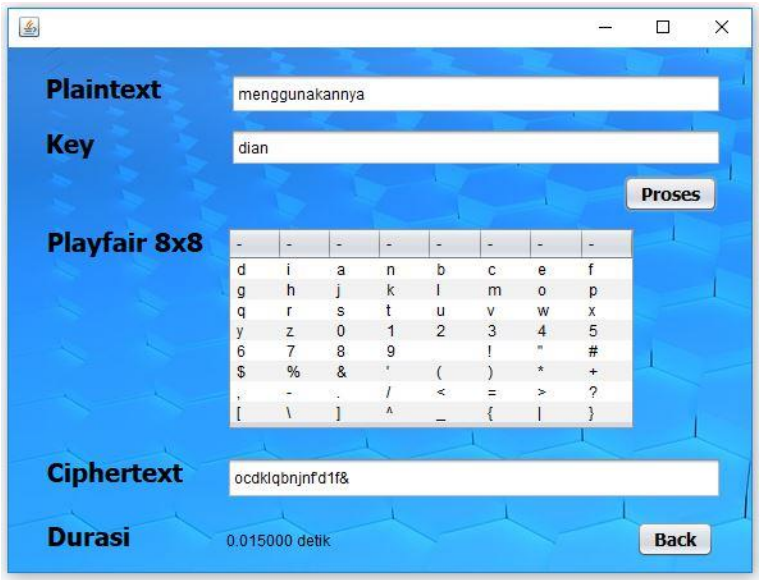
dl : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **dl=ny**.

F& : beda baris beda kolom, maka ambil huruf/karakter dari pertemuan masing-masing huruf/karakter. Jadi **f&=a+**.

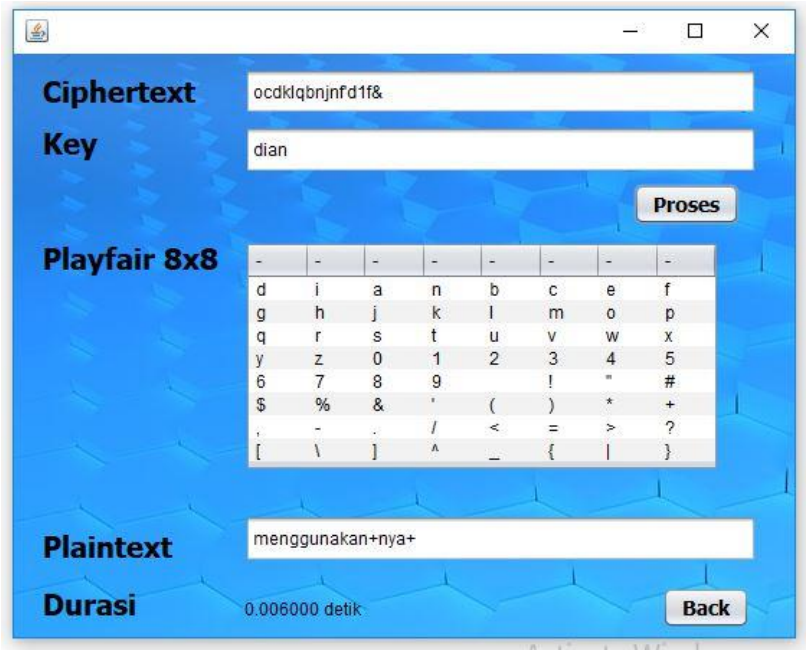
Jadi, oc dk lq bn jn f' dl f& = me ng guna ka n+ ny a+.

Hasilnya yaitu plainteks : menggunakan+nya+

Adapun hasil enkripsi dan dekripsi dari aplikasinya bisa dilihat pada Gambar 4.9 dan Gambar 4.10.



Gambar 3. Hasil Enkripsi



Gambar 4. Hasil Dekripsi

Hasil pembacaandata dari pembahasan layanan keamanan yang berada di bab empat dengan memperhatikan Gambar 4.21 dan Gambar 4.22 bahwa layanan keamanan apa saja yang ada pada program penerapan modifikasi metode *Playfair Cipher* tabel 8x8 dalam penelitian ini.

Tabel 1. Layanan Keamanan

No	Layanan Keamanan	Keterangan
1	*Confidentiality*	Ada
2	*Data Integritas*	Tidak Ada
3	*Authentication*	Ada
4	*Non repudiation*	Tidak Ada

1) Hasil *Pengujian Kunci dan Waktunya*

Dimana dilakukan percobaan tiga kunci dan tiga plainteks yang panjang karakternya berbeda-beda kemudian ketiga palinteks akan di uji dengan ketiga kunci yang ada. Sebagai contoh kita akan menggunakan kunci dan palinteks pada proses enkripsi dan kunci cipherteks pada proses dekripsi di ambil dari hasil proses enkripsi sebagai berikut :

Tabel 2. Tabel palintext

Plaintext	Karakter	Panjang Karakter
1	Dian	4 karakter
2	jika gagal bunuh saja	22 karakter
3	Dunia berkembang kian cepat seiring majunya teknologi informasi. Komunikasi kini menjadi tidak terbatas. Dengan banyaknya kemudahan untuk melakukan pengaksesan informasi, adakalanya diperlukan pengamanan informasi tersebut. Pengamanan ini berfungsi menangani pencegahan atas sampainya informasi ke tangan yang tidak berhak yang dapat menimbulkan kerugian bagi pemilik informasi.	350 karakter

Tabel 3. Tabel *key*

Key	Karakter	Panjang Karakter
1	Coba	4 karakter
2	pilih1&2	8 karakter
3	17agustustahun1945	18 karakter

Tabel 4. Pengujian Durasi Proses Enkripsi

Uji Coba	*Plaintext* 1		*Plaintext* 2		*Plaintext* 3	
	0.000 detik	rata-rata	0.000 detik	rata-rata	0.047 detik	rata-rata
Key 1	0.000 detik	0.005	0.015 detik	0.010	0.015 detik	0.020
	0.015 detik	detik	0.016 detik	detik	0.000 detik	detik
	0.000 detik	rata-rata	0.015 detik	rata-rata	0.047detik	rata-rata
Key 2	0.015 detik	0.01	0.008 detik	0.010	0.031 detik	0.031
	0.015 detik	detik	0.009 detik	detik	0.015 detik	detik
	0.015 detik	rata-rata	0.016 detik	rata-rata	0.093 detik	rata-rata
Key 3	0.000 detik	0.010	0.010 detik	0.014	0.047`detik	0.062
	0.016 detik	detik	0.015 detik	detik	0.047 detik	detik

Tabel 5. Pengujian Durasi Proses Dekripsi

Uji Coba	*Plaintext* 1		*Plaintext* 2		*Plaintext* 3	
	0.015 detik	rata-rata	0.015 detik	rata-rata	0.016 detik	rata-rata
Key 1	0.000 detik	0.005	0.000 detik	0.005	0.015 detik	0.010
	0.000 detik	detik	0.000 detik	detik	0.000 detik	detik
	0.015 detik	rata-rata	0.000 detik	rata-rata	0.016 detik	rata-rata
Key 2	0.000 detik	0.01	0.016 detik	0.010	0.032 detik	0.021
	0.015 detik	Detik	0.015 detik	detik	0.016 detik	detik
	0.016 detik	rata-rata	0.000 detik	rata-rata	0.031 detik	rata-rata
Key 3	0.000 detik	0.010	0.015 detik	0.011	0.032 detik	0.026
	0.015 detik	detik	0.017 detik	detik	0.015 detik	detik

Setelah dilakukan pengujian dari panjang *ciphertext* dan panjang *key* pada proses dekripsi di dapat durasi waktu yang berbeda-beda setiap kali dilakukan penginiputannya maka di tuliskan tiga durasi waktu yang sering berulang kemudian dibagi tiga maka di dapatlah rata-rata durasi waktu prosesnya dimana semakin panjang *key*/kunci yang digunakan maka semakin lama proses enkripsi dan proses dekripsinya, namun pada percobaan ini tidak ada yang melebihi satu detik.

IV. Kesimpulan

Berdasarkan hasil penelitian ini, maka penulis dapat menarik beberapa kesimpulan, yaitu :

1. Hasil pengujian *white box* algoritma yang diterapkan berjalan dengan baik.
2. Layanan Keamanan Data Teks dari hasil pengujian hanya terdapat layanan keamanan *Confidentiality* dan *Authentication*.
3. Jika penggunaan kunci yang digunakan panjangnya lebih pendek maka semakin cepat juga waktu enkripsi dan dekripsinya.

Terdapat karakter baru yang digunakan yaitu karakter *Space*.

Daftar Pustaka

[1] H. Azis, "Network steganography system using covert channel for LSBS stego data on VOIP communication," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 5, pp. 1448–1449, 2019.

[2] H. Azis and F. Fattah, "Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration Testing," *Ilk. J. Ilm.*, vol. 11, no. 2, p. 167, 2019.

[3] A. Djamalilleil, M. Muslim, Y. Salim, E. I. Alwi, H. Azis, and Herman, "Modified Transposition Cipher Algorithm for Images Encryption," *Proc. - 2nd East Indones. Conf. Comput. Inf. Technol.*

Internet Things Ind. EIConCIT 2018, pp. 1–4, 2018.

[4] M. Nazeri, A. Rezai, and H. Azis, "An Efficient Architecture for Golay Code Encoder," *Proc. - 2nd East Indones. Conf. Comput. Inf. Technol. Internet Things Ind. EIConCIT 2018*, pp. 114–117, 2018.

[5] F. Muharram, H. Azis, and A. R. Manga, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," *Pros. Semin. Nas. Ilmu Komput. dan Teknol. Inf.*, vol. 3, no. 2, pp. 112–115, 2018.

[6] Y. Salim and H. Azis, "Metode Digital Watermark Pada File Penelitian Dosen," *Ilk. J. Ilm.*, vol. 9, no. 2, pp. 161–166, 2017.

[7] H. Azis and R. Wardoyo, "Penerapan Network Steganography Menggunakan Metode Modifikasi LACK Dan Layanan Message Authentication Code Pada Voip Network Steganography System with modification of LACK and Message Authentication Code on VoIP," *Semin. Nas. Komun. dan Inform.*, pp. 13–19, 2015.