p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416

Website : jurnal.umj.ac.id/index.php/semnastek

MODIFIKASI ALGORITMA CAESAR CHIPER DAN RAIL FENCE UNTUK PENINGKATAN KEAMANAN TEKS ALFANUMERIK DAN KARAKTER KHUSUS

Retnani Latifah[1*], Sitti Nurbaya Ambo[2], Syafitri Indah Kurnia[3]
[*123]Teknik Informatika , Fakultas Teknik, Universitas Muhammadiyah Jakarta,
Jakarta, Jl Cempaka Putih Tengah 27, 10510
[*]E-mail : retnani.latifah@ftumj.ac.id

ABSTRAK

Saat ini pertukaran data teks secara digital melalui jaringan internet publik telah banyak dilakukan. Salah satu permasalahan yang muncul dari hal tersebut adalah keamanan teks yang dipertukarkan. Metode Caesar Cipher dan Rail Fence adalah metode enkripsi klasik yang dapat digunakan untuk mengamankan pesan teks, namun masih tergolong lemah jika diterapkan sendiri-sendiri. Metode Caesar Cipher terutama memiliki kendala tidak bisa mengamankan teks yang berisi ASCII *printable characters* (alfanumerik dan karakter-karakter khusus). Penelitian ini mengusulkan penggabungan modifikasi Caesar Cipher dan Rail Fence, yaitu dengan menggunakan modulus 95 untuk pergeseran Caesar Cipher karena jumlah ASCII *printable characters* adalah 95 dan menerapkan susunan *reverse order* untuk setiap pembacaan baris hasil penerapan metode Rail Fence. Dari hasil pengujian dengan lima teks berbeda dan kombinasi nilai kunci pergeseran dan kedalaman Rail Fence, diketahui bahwa usulan metode mampu melakukan enkripsi dan dekripsi secara tepat terutama jika nilai kunci pergeseran antara 1-95. *Cipher text* hasil enkripsinya cukup tahan dengan serangan Brute Force karena susunan *cipher text* sudah diacak dengan Rail Fence dan dilakukan *reverse order* untuk setiap barisnya.

Kata kunci: kriptografi, Caesar Cipher, Rail Fence, keamanan teks, modifikasi

ABSTRACT

The exchange of digital text through public network has been done many times. The security of the texts is one of the problems that arises from it. Caesar Cipher and Rail Fence methods are one of classic encryption methods that were used to secure text message but both of them are weak when individually implemented. Especially Caesar Cipher, it has some shortcomings such as it couldn't secure a text which has ASCII printable characters (alphanumeric and special characters). This research proposed a method to combine both Caesar Cipher and Rail Fence, using modulus 95 for Caesar Cipher shifting because ASCII printable characters has 95 characters and implementing reverse order sequence for every row from Rail Fence result. The result of securing five types of text using different shifting key and Rail Fence's depth was the proposed method is able to correctly encrypt and decrypt the texts, especially if the shifting key was range in between 1-95. The resulting cipher text is quite resistance toward Brute Force attack because the sequence of the cipher text has been randomized with Rail Fence and reverse order was implemented in every row.

Keywords : *cryptography, Caesar Cipher, Rail Fence, secure text, modification*

PENDAHULUAN

Dengan semakin banyaknya teks yang dipertukarkan melalui jaringan internet, kebutuhan akan keamanan teks semakin meningkat. Teks-teks yang perlu diamankan biasanya adalah teks pribadi, yang mana pengirimnya tidak ingin isi teksnya diketahui oleh orang lain kecuali orang yang dikirimi teks tersebut. Teks digital, termasuk teks bahasa Indonesia, cenderung tidak hanya berisi huruf alfabet, baik besar maupun kecil, namun juga bisa terdiri dari angka dan karakter-karakter tertentu.

Kriptografi adalah seni tentang bagaimana agar teks menjadi aman dengan cara mengubah teks tersebut menjadi bentuk

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

yang tidak dapat dibaca. Teks yang asli dan masih dapat terbaca disebut sebagai *plain text*, sedangkan teks yang tidak dapat dibaca dan tidak bermakna disebut sebagai *cipher text*. Proses pengubahan *plain text* menjadi *cipher text* disebut sebagai enkripsi (*encryption*), sedangkan proses pengembaliannya disebut sebagai dekripsi (*decryption*). Proses enkripsi digunakan untuk menyembunyikan informasi yang ada di teks dari orang yang tidak diinginkan (Singh, Nandal & Malik, 2012).

Kriptografi dapat diklasifikasikan menjadi tiga tipe yaitu kriptografi dengan kunci simetris, kriptografi dengan kunci asimetris dan kriptografi dengan fungsi hash. Pada kriptografi dengan kunci simetris, pengirim dan penerima teks menggunakan kunci rahasia yang sama untuk melakukan enkripsi dan dekripsi. Teknik ini hanya menerima plaintext yang berisi huruf alfabet, angka dan karakter-karakter khusus. Sedangkan hasil *cipher text* dapat berupa alfabet, angka, karakter khusus maupun kombinasi ketiganya. Teknik kriptografi dengan kunci simetris dapat dikategorikan lagi, yaitu kriptografi klasik dan kriptografi modern (Saranya, Mohanapriya & Udhayan, 2014).

Kriptografi klasik adalah teknik kriptografi yang telah dikembangkan dari zaman terdahulu, bahkan sebelum komputer ditemukan. Meskidemikian, sampai saat ini teknik kriptografi klasik masih digunakan untuk mengamankan informasi (Saranya, Mohanapriya & Udhayan, 2014). Kriptografi klasik masih dapat dibagi lagi menjadi *cipher* substitusi (*substitution cipher*) dan *cipher* transposisi (*transpotition cipher*). *Cipher* substitusi adalah algoritma kriptografi yang mengganti setiap unit *plain text* dengan satu unit *cipher text*. Sedangkan *cipher* transposisi adalah mengubah urutan huruf *plain text* atau melakukan *transpose* terhadap rangkaian karakter (Setyaningsih, 2015).

Salah satu metode yang termasuk *cipher* substitusi adalah metode Caesar Cipher. Metode Caesar Cipher adalah salah satu metode yang paling lama dan paling sederhana (Dar, 2014). Metode ini ditemukan di abad ke-19 oleh Julius Caesar saat Caesar akan mengirimkan pesan kepada jenderalnya, namun kurir pesannya tidak dapat dipercaya. Caesar kemudian mengubah setiap huruf A menjadi huruf D, setiap huruf B menjadi huruf E dan seterusnya. Orang yang dapat menterjemahkan pesan tersebut hanyalah orang-orang yang mengetahui bahwa kunci pergeserannya adalah 3 (Singh, Nandal & Malik, 2012).

Caesar Cipher adalah salah satu teknik sederhana enkripsi yang mengganti setiap karakter alfabet dengan karakter lain dengan panjang alfabet sejumlah 26 (Setyaningsih, 2015). Secara umum rumus enkripsi dan dekripsi Caesar Cipher adalah sebagai berikut (Dar, 2014) :

Enkripsi :

$$E(x)= x + K \bmod 26 \quad (1)$$

Dekripsi :

$$D(x)= x – K \bmod 26 \quad (2)$$

dimana K adalah nilai kunci yang digunakan untuk menggeser setiap karakter x.

Misal ingin melakukan enkripsi plaintext yang berisi HALO APA KABAR dengan kunci 3, maka huruf H diganti dengan huruf K, huruf A diganti dengan huruf D, huruf L diganti dengan huruf O dan seterusnya. Hasil ciphertext akan beisi KDOR DSD NDEDU.

Metode ini memiliki kelemahan yaitu orang lain yang tidak berwenang akan dapat memecahkan *cipher text* dengan menggunakan metode Brute force dengan cara mencoba semua kunci (Singh, Nandal & Malik, 2012) maupun dengan mencocokkan distribusi frekuensi dari huruf yang muncul. Distribusi huruf dalam bahasa Inggris mudah untuk dibedakan dan diprediksi (Jain, Dedhia & Patil, 2015).

Metode enkripsi Rail Fence adalah salah satu bentuk *cipher* transposisi yang sederhana yang diinspirasi dari model *Polybius square*. *Polybius square* adalah menyusun huruf sebagai matriks 5x5 dan mengkodekan huruf A sebagai 1-1, huruf B sebagai 1-2 dan seterusnya. Setiap karakter pada *Polybius square* diganti dengan indeks *cell* matriks tanpa menggunakan kunci khusus dan hanya merubah posisi sehingga teks tidak terbaca. Berbeda dengan *Polybius square*, metode Rail Fence menyusun teks secara zig-zag yang model matriksnya diketahui oleh pengirim dan penerima pesan (Siahaan, 2016).

Studi oleh Singh dkk (2012) menyebutkan bahwa teknik Rail Fence adalah menuliskan plaintext dalam urutan diagonal dan membacanya sebagai urutan baris sehingga terbentuk ciphertext. Contohnya jika

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

ingin mengenkripsi HALO APA KABAR maka spasi dihilangkan kemudian disusun diagonal membentuk pola zig-zag. Misal ingin dibuat dengan kedalaman (jumlah baris) 3, maka hasil perubahan susunannya adalah sebagai berikut :

H				A				A			
	A		O		P		K		B		R
		L				A				A	

Hasil *cipher text* : HAA AOPKBR LAA .

Metode Rail Fence mudah untuk dibobol oleh kriptanalis dengan mencoba beberapa nilai kedalaman untuk menentukan banyaknya baris yang digunakan. Terdapat pola tertentu berdasarkan jumlah baris yang digunakan. Misal jika ada dua baris maka huruf ke 1,3,5,... akan berada di baris pertama dan huruf ke 2,4,6,... akan ada di baris kedua (Singh, Nandal & Malik, 2012). Meskipun metode Rail Fence adalah metode yang lemah, namun metode ini dapat digabungkan dengan metode lain untuk meningkatkan keamanan *cipher text* sehingga tidak mudah dipecahkan (Siahaan, 2016).

Salah satu studi yang telah dilakukan adalah menggabungkan metode Rail Fence dengan metode Caesar Cipher. Pada studi tersebut, proses enkripsi *plain text* dilakukan dengan menerapkan Caesar Cipher terlebih dahulu kemudian pada ciphertext tersebut diterapkan metode Rail Fence. Hasil dari studi tersebut adalah *cipher text* yang dihasilkan lebih sulit untuk dilakukan kriptanalis, tidak dapat dengan mudah dilakukan rekronstruksi, Brute Force tidak bisa membobol kode *cipher* dan secara keseluruhan mengatasi kekurangan Caesar Cipher (Singh, Nandal & Malik, 2012).

Contoh penerapan metodenya adalah sebagai berikut :

Proses Enkripsi

1. *Plain text* adalah HALO APA KABAR. Setelah spasinya dihilangkan menjadi HALOAPAKABAR
2. Misal kunci yang dipakai adalah 3, dengan Caesar Cipher pesan akan menjadi KDORDSDNDEDU
3. Tuliskan hasil dari 2 menjadi urutan diagonal dan baca menjadi baris

K O D D D D
D R S N E U

Terbaca sebagai KODDDD DRSNEU

4. Lakukan PUSH kata pada 2 *stack* yang berbeda sehingga menjadi

D	U
D	E
D	N
D	S
O	R
K	D

5. Lakukan POP pada setiap *stack* sehingga *cipher text* akhir adalah DDDDOK UENSRD

Proses Dekripsi

1. PUSH *cipher text* ke *stack* sesuai masing-masing kata

K	D
O	R
D	S
D	N
D	E
D	U

2. Lakukan POP dari bagian atas *stack* pertama dan *stack* kedua sehingga terbentuk kata KD
3. Ulangi untuk isian *stack* selanjutnya sehingga terbentuk KDORDSDNDEDU
4. Gunakan rumus dekripsi Caesar Cipher sesuai dengan rumus (2) sehingga ketemu teks HALOAPAKABAR

METODE

Metode yang diusulkan oleh Singh dkk (2012) sudah mampu untuk mengatasi kekurangan dari Caesar Cipher termasuk jika diserang menggunakan algoritma Brute Force. Namun, usulan metode tersebut hanya untuk huruf-huruf besar. Selain itu, Rail Fence yang digunakan hanya menggunakan dua baris sehingga hasil *cipher text* akan selalu menjadi dua kata.

Pada penelitian ini dilakukan modifikasi metode yang telah dikembangkan oleh Singh dkk agar metode tersebut dapat melakukan enkripsi teks yang terdiri dari huruf besar, huruf kecil, angka dan karakter-karakter khusus. Modifikasi lain juga dilakukan pada metode Rail Fence dimana kedalaman dari Rail Fence bisa tergantung keinginan pengirim dan penerima.

Modifikasi Caesar Cipher Proses Enkripsi

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Modifikasi yang dilakukan adalah tidak melakukan pembuangan spasi pada *plain text* dan modulus yang digunakan adalah modulus 95 karena terdapat 95 karakter yang digunakan, yaitu dari karakter nomor 32 dalam tabel ASCII sampai karakter 126 atau disebut sebagai ASCII *printable characters* seperti yang ditunjukkan pada gambar 1.

Berikut adalah rumus modifikasi enkripsi Caesar Cipher yang diterapkan :

$E(x) = ((x – spasi + k) \bmod 95) + spasi$ (3)

dimana x adalah karakter yang akan diganti dan k adalah nilai kunci. Spasi adalah nomor ASCII dari karakter spasi.

Pengurangan nomor ASCII karakter x dengan nomor ASCII spasi dilakukan untuk melakukan normalisasi perhitungan sehingga interval angka karakter bukan 32-126 melainkan dari 0-95. Fungsi penambahan nomor karakter spasi setelah dilakukan modulus adalah agar nilai E(x) kembali berada di interval 32-126.

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Gambar 1. ASCII printable characters

Misal *plain text* yang akan dienkripsi adalah ”Halo, Apa Kabar?~” (tidak termasuk tanda kutip) dengan kunci pergeseran 3. Beberapa hasil enkripsinya adalah :

- H : ((72-32+3) mod 95)+32 = 75 → K
- a : ((97-32+3) mod 95)+32 = 100 → d
- , : ((44-32+3) mod 95)+32 = 47 → /
- spasi : ((32-32+3) mod 95)+ 32 = 35 → #
- ~ : ((126-32)+3) mod 95)+32 = 34 → ”

Dengan demikian *cipher text* hasil penerapan modifikasi Caesar Cipher menjadi Kdor/#Dsd#NdeduB"

Modifikasi Rail Fence Proses Enkripsi

Pada proses Rail Fence, modifikasi yang dilakukan adalah kedalaman atau jumlah baris dapat ditentukan oleh pengirim pesan. Setelah dilakukan penyusunan *cipher text* hasil Caesar Cipher secara zig-zag berdasarkan kedalaman dan dibaca per baris, setiap kata yang terbentuk kemudian dilakukan *reverse order* dan disusun menjadi satu diberi spasi untuk pembeda setiap baris.

Misal dengan menggunakan kedalaman 3, *cipher text* hasil Caesar Cipher akan disusun menjadi berikut

K / d e ”
d r # s # d d B
o D N u

- Baris pertama diperoleh K/de”
- Baris kedua diperoleh dr#s#ddB
- Baris ketiga diperoleh oDNu

Setiap baris dilakukan *reverse order* :

- Baris pertama menjadi ”ed/K
- Baris kedua menjadi Bdd#s#rd
- Baris ketiga menjadi uNDo

Dengan demikian *cipher text* akhir adalah ”ed/KBdd#s#rduNDo

Modifikasi Dekripsi

Proses dekripsi diawali dengan membalikkan *reserve order* untuk setiap baris Rail Fence dan kemudian melakukan dekripsi Caesar Cipher. Langkah-langkah yang dilakukan adalah :

1. Membuat Rail Fence dengan tingkat kedalaman yang sama seperti di enkripsi untuk mengetahui jumlah karakter yang ada di setiap baris.

”				K				#				d				o
	e		/		B		d		s		r		u		D	

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

		d				d				#				N		

- Jumlah karakter di baris pertama : 5
- Jumlah karakter di baris kedua : 8
- Jumlah karakter di baris ketiga : 4

2. Setelah mengetahui jumlah karakter di setiap baris Rail Fence, pecah *cipher text* menjadi sebanyak baris dengan jumlah setiap barisnya sesuai yang ditemukan di langkah 1.
   - Baris pertama berisi : ”ed/K
   - Baris kedua berisi : Bdd#s#rd
   - Baris ketiga berisi : uNDo
3. Lakukan *reverse order* di setiap baris dan susun menjadi satu
   K/de”dr#s#ddBoDNu (sama seperti hasil enkripsi setelah dilakukan Rail Fence)
4. Terapkan proses dekripsi Rail Fence : Kdor/#Dsd#NdeduB”
5. Lakukan dekripsi Caesar Cipher dengan rumus dekripsi sebagai berikut :
   D(x) =
   ((95+x-spasi-kunci) mod 95)+spasi (4)

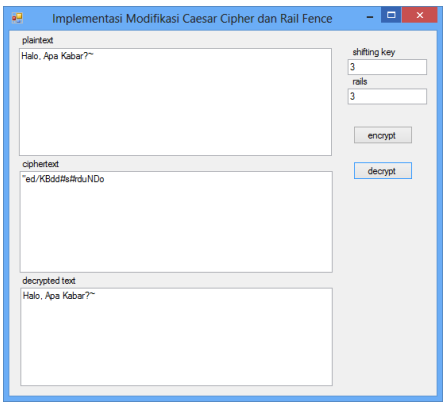
   Penambahan angka 95 ditujukan agar hasil modulus yang diperoleh adalah benar sesuai dengan karakter di *plain text*. Jika tidak ditambah dengan angka 95, maka hasil modulusnya tidak sesuai yang menyebabkan kegagalan dekripsi. Berikut adalah beberapa hasil dekripsi dari teks di langkah keempat :
   - K : ((95+75-32-3) mod 95)+32 = 72 → H
   - d : ((95+100-32-3) mod 95)+32 = 97 → a
   - / : ((95+47-32-3) mod 95)+32 = 44 → ,
   - #:((95+35-32-3) mod 95)+32 = 32 → spasi
   - ”:((95+34-32-3) mod 95)+32 = 126 → ~

Hasil akhir dekripsi adalah Halo, Apa Kabar?~

HASIL DAN PEMBAHASAN

Metode yang telah dipaparkan di subbab sebelumnya diimplementasikan dengan menggunakan bahasa pemrograman C#, dimana pengguna dapat menentukan kunci pergeseran Caesar Cipher yang digunakan dan nilai kedalaman Rail Fence. Hasil implementasi dapat dilihat di Gambar 2.

Pengujian dilakukan dengan 5 tipe teks yang berbeda, yang mana nilai kunci dan banyaknya baris Rail Fence diganti-ganti untuk dapat mengetahui apakah metode yang diusulkan mampu melakukan enkripsi dan dekripsi dengan tepat untuk teks apapun dan dengan nilai kunci pergeseran dan kedalaman Rail Fence berapapun. Teks-teks yang diuji dapat dilihat di Tabel 1.



Gambar 2. Tampilan Implementasi Modifikasi Caesar Cipher dan Rail Fence

TABEL 1. Teks Untuk Pengujian

1	CORELDRAW GRAPHICS SUITE X7 PURCASE SERIAL NUMBER: DR17R20-EWGSH43-U5UW9TS-KGXNQME ACTIVATION CODE: CFF2-2337-87A6-4909-8507
2	Caesar Cipher Merupakan Teknik Kriptografi Dan Enkripsi Yang Sudah Ada Sejak Zaman Julius Caesar. Cipher Ini Dirancang Sendiri Oleh Julius Caesar Cipher Untuk Mengirim Pesan Kepada Cleopatra. Enkripsinya Menggunakan Teknik Penggeseran Karakter 3 Langkah Ke Kiri Dari Karakter A-Z.
3	Jadi, untuk setiap cipher, penggeseran karakter ke-i pada alfabet menjadi karakter ke i+k pada urutan alfabet inilah yang disebut caesar cipher.

4	foreach (char c in plainText)
	{
	int ascii = (int)c;
	int space = (int)' ';
	cc = ((ascii - space + kunci) % 95) + space;
	char hs = (char)cc;
	hasil += hs;
	}

5	K : ((95+75-32-3) mod 95)+32 = 72

Pengujian dilakukan beberapa kali dengan menggunakan kelima teks yang ada di Tabel 1. Dari beberapa kali pengujian tersebut, ditampilkan 11 hasil pengujian yang dapat dilihat di Tabel 2. Dari hasil pengujian, diketahui bahwa metode yang diusulkan mampu untuk melakukan enkripsi dan dekripsi secara tepat untuk berbagai tipe teks, terutama jika nilai kunci pergeseran yang digunakan adalah dalam range 1-95.

Metode yang diusulkan juga mampu untuk melakukan enkripsi dan dekripsi dengan nilai kunci diatas 95, meskipun tidak semua angka dapat digunakan seperti yang dapat

dilihat dari percobaan ke-3 dan ke-11. Pada percobaan ke-11 dengan teks berisi alfanumerik dan karakter dimana alfabetnya adalah berupa huruf besar, metode yang diusulkan sukses melakukan dekripsi. Namun pada percobaan ke-11, dekripsi gagal karena ada satu karakter yang tidak terdekripsi dengan benar.

Percobaan ke-8 dan ke-9 dikatakan kurang sukses karena metode tidak melakukan dekripsi secara tepat yaitu karakter pindah paragraf dan tab tidak mampu didekripsi karena memang tidak termasuk karakter ASCII yang dapat didefinisikan di usulan metode. Setiap karakter pindah paragraf dan tab didekripsikan sebagai li dan h sehingga dapat dikatakan bahwa proses dekripsi berjalan dengan tepat.

Secara umum dapat diketahui bahwa metode yang diusulkan dapat melakukan enkripsi dan dekripsi secara tepat untuk beberapa tipe teks jika nilai kunci pergeseran antara 1-95. Sedangkan untuk nilai kedalaman Rail Fence, metode mampu menerima nilai Rail sampai 20 dan dapat terenkripsi dan dekripsi secara tepat jika nilai kunci sesuai.

Ciphertext hasil enkripsi tidak dapat dibobol dengan mudah dengan menggunakan algoritma Brute Force karena walaupun nilai kunci dan kedalaman sudah benar, hasil dekripsinya akan salah karena pada tahap enkripsi di usulan metode dilakukan *reverse order* untuk setiap baris Rail Fence.

Tabel 2. Hasil Pengujian Metode Modifikasi Caesar Cipher dan Rail Fence

<table>
<tr><th>No</th><th>Teks</th><th>Key</th><th>Rail</th><th>Enkripsi</th><th>Dekripsi</th><th>Hasil</th></tr>
<tr><td>1</td><td>Ke-1</td><td>9</td><td>4</td><td>ciphertext
A6@OMRLW]6`@[]₩[])J[L>6=?6<;ONXX]]JZa₩B^<PN[:CNWUN)L^aN₩₩Y<br>[JMX9BBJA<6LCLWJR)VP6`>=₩6;[)K^J[NJY@]^LQP`U[@9@;))_NT^Q9MVR
₩)RR)N</td><td>decrypted text
CORELDRAW GRAPHICS SUITE X7 PURCASE SERIAL NUMBER: DR17R20
-EWGSH43-U5UW9TS-KGXNQME ACTIVATION CODE: CFF2-2337-87A6-4909
-8507</td><td>Sukses</td></tr>
<tr><td>2</td><td>Ke-1</td><td>73</td><td>7</td><td>ciphertext
"!.->A<=i+-~vvl/9>+=#1/$//iB/:<9y#"|$-3ivA=vi,</!>21<!y!{ii@/5?2y.73=i33i/#
+v-8+71~}{<?++:?-A6} {09>;B?|<z86-?==+.v038v!i<i<</td><td>decrypted text
CORELDRAW GRAPHICS SUITE X7 PURCASE SERIAL NUMBER: DR17R20
-EWGSH43-U5UW9TS-KGXNQME ACTIVATION CODE: CFF2-2337-87A6-4909
-8507</td><td>Sukses</td></tr>
<tr><td>3</td><td>Ke-1</td><td>124</td><td>12</td><td>ciphertext
U^Jrq`TJqsrPjkbfl^TffRQ_==roSPlqrebiupbJPk`tpo^T=iQO=^VdWf=paVJ`=qt=om`
oMOlbpbabrf^VcajJJopoetTJcbnhMN=`m=MU`WkdOTb^^dR=uopo</td><td>decrypted text
CORELDRAW GRAPHICS SUITE X7 PURCASE SERIAL NUMBER: DR17R20
-EWGSH43-U5UW9TS-KGXNQME ACTIVATION CODE: CFF2-2337-87A6-4909
-8507</td><td>Sukses</td></tr>
<tr><td>4</td><td>Ke-2</td><td>25</td><td>6</td><td>ciphertext
z#%.~#((G9-~~z"~#*₩z99, 9%"₩G%,9,z!~%,-%(z/3#9z₩zz~(f,"~₩9~(l,]"#z9
(!zl!#%#zd%zz~*zs.z]#"(,zz~9%%!z-^,&}(i!99*-9c&}9z9~₩~-9z~}/(*(9,,#
(*,#~F~dzd9z9,(!i~z!9*(.~z99#%n#z-/h#!(#,9-/cs$Z}z-^]!#(9/9₩-Z,9,9deLz9!~m
((f#%z)*d',/(₩,/&9,(|(9Gz#/9z9zr#9z)*%m,f9z9#~9d(9~,*~#.9##zb,&%"9(.~~,</td><td>decrypted text
Caesar Cipher Merupakan Teknik Kriptografi Dan Enkripsi Yang Sudah Ada Sejak
Zaman Julius Caesar. Cipher Ini Dirancang Sendiri Oleh Julius Caesar Cipher
Untuk Mengirim Pesan Kepada Cleopatra. Enkripsinya Menggunakan Teknik
Penggeseran Karakter 3 Langkah Ke Kiri Dari Karakter A-Z.</td><td>Sukses</td></tr>
<tr><td>5</td><td>Ke-2</td><td>25</td><td>18</td><td>ciphertext
.zf-/~}*₩~%%,~9z~-#,"zZ.#z,z.z(z(i9&9*99),~9,~d!399₩/b#l"!d-Zz,9!(d'zc
(₩~z,9zFd9(/#~#~9#9$}z%,s9Lz(-*,-"9Gz/ #9G#9,z*z#z~],%l#(₩,e~
%#}!,&#z999%#zz-z,z(9h,-s!]~*](~(%9~₩9z~z(zm"9!!9(₩f##(z'z(9~#%!m^&9*,l
₩zr9(,,z(~9~%"#z9(9^z9#"~%G)/~}(-9#(%fd9i(z*.,(!/c-%z~9d9#,z(9~9#/*,*,~
%.nl&#/</td><td>decrypted text
Caesar Cipher Merupakan Teknik Kriptografi Dan Enkripsi Yang Sudah Ada Sejak
Zaman Julius Caesar. Cipher Ini Dirancang Sendiri Oleh Julius Caesar Cipher
Untuk Mengirim Pesan Kepada Cleopatra. Enkripsinya Menggunakan Teknik
Penggeseran Karakter 3 Langkah Ke Kiri Dari Karakter A-Z.</td><td>Sukses</td></tr>
<tr><td>6</td><td>Ke-3</td><td>56</td><td>5</td><td>ciphertext
XM@B?
KD>BM:D:>K:M#f<KXNXGEG:ENNXcKMX=X>X=>XKDL@d>IBNG:KB:<;=::B;:M
XIBXDD:F;::eK:X>@XAXMDN=>IL:>BRAX>X:::XD::C>:EIB>DGKGII<>XXBA>LX
MG=>KG?XM:>BLd</td><td>decrypted text
Jadi, untuk setiap cipher, penggeseran karakter ke-i pada alfabet menjadi
karakter ke i+k pada urutan alfabet inilah yang disebut caesar cipher.</td><td>Sukses</td></tr>
<tr><td>7</td><td>Ke-3</td><td>56</td><td>20</td><td>ciphertext
:KX#AE::DG:XBDD::=RGMXKKB:B>B:>dGXK=DLX@MX:M>NX>DC>@G=;>GK
@MfB:X>XGNKL?
BFD>D>>EcX>IXA;:DMeXLINXX>Bd>BMGI;XKM<X:::I>BX<M=?:A:K:N:E=II:>KX:
:BXLNX<</td><td>decrypted text
Jadi, untuk setiap cipher, penggeseran karakter ke-i pada alfabet menjadi
karakter ke i+k pada urutan alfabet inilah yang disebut caesar cipher.</td><td>Sukses</td></tr>
<tr><td>8</td><td>Ke-4</td><td>9</td><td>3</td><td>ciphertext
'l4(‼lqF)lDy))rtn|rjF↨0}|l)↨lr)lw┬2]ur{1jo┬‼DqF)rj↨┬l2jl))q{q↨┬nj|42B.2l~))ly))r|
1))l‼D)2w1Fnj|}r‼D2w1Frlj}r‼%┬}nwjyw))jl)lnx‼┬)uqD{1|
|‼l)>)w4j6l1l┬0r)yw┬})r)↨‼"r)lqq{</td><td>decrypted text
foreach (char c in plainText)li{lihint ascii = (int)c;lihint space = (int)' ';lihcc = ((ascii -
space + kunci) % 95) + space;lihchar hs = (char)cc;lihhasil += hs;li}li</td><td>Kurang sukses</td></tr>
<tr><td>9</td><td>Ke-4</td><td>78</td><td>20</td><td>ciphertext
b$unUXPw(*nPc^[Wnn[ub]anWysXwRXTyXnnWcXWP,[bwR]XXRn*_XRXn
[WWRPRnv,jnbRR],nnXv*wTdn,v[R[a*ZvnXwWXP[nvT]cPlWXyPRcga
[RWnbPwTnXvRTR_RCRnWRXb*]n,PPXn[XXna_ncXP]bnb{]W[nWnX_</td><td>decrypted text
foreach (char c in plainText)li{lihint ascii = (int)c;lihint space = (int)' ';lihcc = ((ascii -
space + kunci) % 95) + space;lihchar hs = (char)cc;lihhasil += hs;li}li</td><td>Kurang sukses</td></tr>
<tr><td>10</td><td>Ke-5</td><td>78</td><td>20</td><td>ciphertext
:n)nvv!(&$ny,&n$!{""y!w{$"(wnnS₩^</td><td>decrypted text
K : ((95+75-32-3) mod 95)+32 = 72</td><td>Sukses</td></tr>
<tr><td>11</td><td>Ke-5</td><td>124</td><td>3</td><td>ciphertext
O=F"FPHEhTZOHR=-=POJTRE===PV+JRVW</td><td>decrypted text
K : ((95+75-32-3) [illegible] | 95)+32 = 72</td><td>Gagal</td></tr>
</table>

SIMPULAN DAN SARAN

Metode Caesar Cipher dan Rail Fence adalah metode kriptografi klasik yang cukup lemah jika diterapkan sendiri-sendiri, namun akan lebih kuat jika digabung. Penelitian ini mengusulkan penggabungan metode Caesar Cipher dan Rail Fence untuk mengamankan teks alfanumerik dan karakter khusus ASCII printable characters. Metode Caesar Cipher menggunakan modulus 95 dengan sedikit perubahan rumus di enkripsi dan dekripsi. Selain itu pada setiap baris Rail Fence juga dilakukan reverse order untuk melakukan pengacakan urutan sehingga *cipher text* tidak dengan mudah dipecahkan oleh pihak yang tidak diinginkan.

Hasil pengujian dengan 5 teks yang berbeda dan kombinasi beberapa nilai kunci pergeseran dan kedalaman menunjukkan bahwa usulan metode secara umum mampu

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

melakukan enkripsi dan dekripsi secara tepat, terutama jika kunci antara 1-95. Penelitian selanjutnya diharapkan dapat mengatasi permasalahan salah dekripsi jika kunci lebih dari 95 dan dapat melakukan kriptografi untuk karakter ASCII yang lain.

DAFTAR PUSTAKA

Dar, S.B. 2014. Enhancing the Security of Caesar Cipher Using Double Substitution Method. *International Journal of Computer Science & Engineering Technology (IJCSET)*. Vol 5, No. 07.

Jain, A., Dedhia., R. & Patil, A. 2015. Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication. *International Journal of Computer Application*. Vol 129, No. 13.

Kurnia, S.I. 2017. *Implementasi Algoritma Caesar Cipher* dalam Pengamanan Pesan. Skripsi tidak diterbitkan. Jakarta : Teknik Informatika UMJ

Saranya, K., Mohanapriya, R. & Udhayan, J. 2014. A Review on Symmetric Key Encryption Techniques in Cryptography. *International Journal of Science, Engineering and Technology Research (IJSETR)*. Vol 3, Issue 3.

Setyaningsih, E. 2015. *Kriptografi & Implementasinya Menggunakan Matlab*. Yogyakarta : Penerbit Andi.

Siahaan, A.P.U. 2016. Rail Fence Cryptography in Securing Information. *International Journal of Science & Engineering Research (IJSER)*. Vol 7, Issue 7.

Singh, A. Nandal, A. & Malik, A. 2012. Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*. Vol 2, Issue 12.

Krisna, I.M. 2011. Rail Fence Cipher C# Source Code. http://www.imkrisna.com/blog/2011/01/rail-fence-cipher-c-source-code-2/ (diakses tanggal 29 September 2017)