

## APLIKASI KRIPTOGRAFI BERBASIS ANDROID MENGUNAKAN ALGORITMA CAESAR CIPHER DAN VIGENERE CIPHER

Imam Wahyu Utomo<sup>1</sup>, Retnani Latifah<sup>2</sup> dan Rita Dewi Risanty<sup>3</sup>

<sup>1,2,3</sup>Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jakarta,  
Jl Cempaka Putih Tengah 27, 10510, Jakarta

wahyuimam09@gmail.com

### Abstrak

Kriptografi adalah suatu cara yang dapat digunakan untuk menjaga kerahasiaan dan keamanan informasi dari orang yang tidak berkepentingan. Metode *caesar cipher* dan *vigenere cipher* adalah metode enkripsi klasik yang tergolong lemah bila diterapkan masing-masing. Penelitian ini mengusulkan penggabungan metode *caesar cipher* dan *vigenere cipher*, yaitu dengan menggunakan *modulus 94* untuk pergeseran *caesar cipher* karena jumlah ASCII character yang digunakan adalah 94 dan menggunakan 94 ASCII character untuk membuat tabel *vigenere*. Dari hasil pengujian dengan 4 teks uji yang berbeda dan kombinasi kunci *caesar* dan *vigenere* yang berbeda pula dapat diketahui bahwa usulan metode dapat melakukan enkripsi dan dekripsi dengan tingkat kesuksesan 0,75. Yang perlu diperhatikan adalah pemakaian karakter yang tepat agar proses enkripsi dan dekripsi dapat berjalan dengan optimal, karena jika karakter yang dipakai berada di luar batasan karakter yang digunakan maka karakter tersebut tidak dapat dienkripsi dan dekripsi. Penelitian ini menghasilkan aplikasi untuk melakukan enkripsi dan dekripsi teks berbasis android sehingga dapat digunakan di mana saja.

**Kata Kunci** : kriptografi, *caesar cipher*, *vigenere cipher*, keamanan informasi, android

### Abstract

*Cryptography is a way to maintain the confidentiality and security of information from unauthorized persons. Caesare cipher and vigenere cipher are classical encryption methods which are relatively weak when applied individually. This study proposes the incorporation of caesar cipher and vigenere cipher method, using modulus 94 for caesarean section shift because the ASCII character that were used are 94. This study also used 94 ASCII character to create vigenere table. From the test results with 4 different test texts and different combinations of caesar and vigenere keys it can be seen that the proposed method can encrypt and decrypt with 0.75 successful rate. The thing that need to be note is the use of the right character for the encryption and decryption process so it can run optimally. Because if the characters used are outside the character limit then the characters can not be encrypted and decrypted. This study produces an application in android based that can be used to encrypt and decrypt text everywhere..*

**Keywords** : *cryptography, caesar cipher, vigenere cipher, information security, android*

### PENDAHULUAN

Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut aspek-aspek keamanan, kepentingan umum dan kepentingan pribadi. Informasi-informasi

tersebut tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya. Salah satu cara mengamankan informasi, terutama

informasi berupa teks adalah dengan kriptografi.

Kriptografi merupakan ilmu mengenai metode untuk mengirimkan pesan secara rahasia sehingga hanya penerima yang dimaksud yang dapat menghapus dan membaca pesan tersebut atau memahaminya (Prayitno & Nurdin, 2017). Kriptografi dapat dibagi menjadi dua kategori yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik merupakan kriptografi yang sudah dikembangkan bahkan sejak belum ada komputer. Beberapa metode kriptografi klasik adalah *substitution cipher* dan *transposition cipher* (Saranya, Mohanapriya, & Udhayan, 2014). Salah satu metode kriptografi berbasis *substitution cipher* adalah algoritma Caesar cipher dan Vigenere cipher (Saputra, Hasibuan, Mesran, & Rahim, 2017).

*Caesar Cipher* merupakan teknik enkripsi substitusi yang pertama kali dikenal dan paling sederhana, yang ditemukan oleh Julius Caesar. Metode yang digunakan dalam *Caesar cipher* ini adalah dengan mempertukarkan setiap huruf asli (*plain text*) dengan huruf lain menggunakan interval 3 sehingga membentuk suatu *cipher text* (Rahim, 2016). Caesar cipher merupakan salah satu teknik sederhana yang mengganti setiap karakter alfabet dengan karakter lain sepanjang 26 karakter alfabet (Setyaningsih, 2015). Rumus enkripsi dan dekripsi dari Caesar cipher adalah sebagai berikut (Rahim, 2016) :

$$C = E(P) = (P + K) \text{ mod } 26 \quad (1)$$

$$P = D(C) = (C - K) \text{ mod } 26 \quad (2)$$

C adalah cipher text, P adalah plain text dan K adalah nilai kunci yang digunakan untuk mengganti setiap karakter.

Algoritma Caesar cipher mengalami beberapa modifikasi, salah satunya adalah mengganti modulus yang digunakan dari 26 menjadi 256 untuk dapat digunakan di semua karakter ASCII (Prayitno & Nurdin, 2017). Selain itu ada juga yang mengganti dengan modulus 95 dikarenakan karakter ASCII yang digunakan adalah karakter dari indeks 32 sampai 126. Selain mengganti modulusnya, pada penelitian tersebut juga dilakukan perubahan rumus (Latifah, Ambo, & Kurnia, 2017). Selain kedua penelitian

tersebut, algoritma Caesar cipher sudah cukup sering dilakukan modifikasi untuk meningkatkan keamanan.

Algoritma Vigenere cipher merupakan algoritma yang lebih kuat dibandingkan dengan Caesar cipher (Saputra, Hasibuan, Mesran, & Rahim, 2017). *Vigenere cipher* merupakan pengembangan dari *Caesar cipher*, namun pada Sandi *Vigenere* terdiri dari beberapa sandi *Caesar* dengan nilai geseran yang berbeda. Tabel *Vigenere* berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 kemungkinan sandi *Caesar*. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang (Kusumawardani, 2010). Gambar 1 menunjukkan tabel *Vigenere cipher*.

Rumus enkripsi dan dekripsi pada Vigenere cipher adalah sebagai berikut (Saputra, Hasibuan, Mesran, & Rahim, 2017):

$$C_i = (P_i + K_i) \text{ mod } 26 \quad (3)$$

$$P_i = (C_i - K_i) \text{ mod } 26 \quad (4)$$

$C_i$  adalah cipher text dari  $C_0$  sampai  $C_n$ ,  $P_i$  adalah plain text dari  $P_0$  sampai  $P_n$  dan  $K_i$  adalah kunci dari  $K_0$  sampai  $K_n$ . Jika menggunakan semua karakter ASCII maka modulus diganti dengan 256.

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

Gambar 1. Tabel Vigenere 26 x 26

### METODOLOGI PENELITIAN

Pada penelitian ini akan dilakukan penggabungan metode Caesar cipher dan Vigenere cipher. Meskipun, Vigenere cipher sendiri adalah pengembangan dari metode

Caesar cipher, pada penelitian ini ingin diketahui bagaimana hasil enkripsi dan dekripsi jika dilakukan algoritma Caesar cipher terlebih dahulu kemudian algoritma Vigenere. Penerapan metode *Caesar cipher* dan *Vigenere cipher* disini menggunakan 94 karakter, yaitu karakter ASCII dengan nomor indeks antara 32 sampai 125.

Rumus enkripsi dan dekripsi Caesar cipher yang digunakan pada penelitian ini adalah sebagai berikut :

$$C = (P+K) \text{ mod } 94 \tag{5}$$

$$P = (C-K) \text{ mod } 94 \tag{6}$$

Untuk proses dekripsi, rumus di atas hanya digunakan saat indeks cipher lebih besar atau sama dengan kunci yang digunakan ( $C \geq K$ ). Jika indeks cipher lebih dari kunci ( $C < K$ ) maka digunakan rumus berikut :

$$P = (C+94-K) \text{ mod } 94 \tag{7}$$

Perbedaan penggunaan formula ini digunakan untuk menyesuaikan pergeseran nilai karakter dengan kunci yang digunakan. Contoh jika indeks cipher adalah 50 dan kunci 70, maka jika menggunakan formula (6) hasil yang didapat akan bernilai negatif dan keluar dari jangkauan indeks karakter. Hal tersebut menyebabkan proses dekripsi tidak dapat dilaksanakan. Oleh karena itu

digunakan formula (7) agar hasil menjadi positif dan dekripsi dapat dilakukan dengan benar.

Contoh penerapan Caesar cipher adalah sebagai berikut :

Plain text : "Tugas\_2017!." (karakter "" tidak termasuk yang dienkripsi)

kunci : 50

Indeks huruf "T" adalah 52, sehingga hasil enkripsi adalah  $C = (52+50) \text{ mod } 94 = 8$ , yaitu karakter "(" . Setelah semua karakter dienkripsi, maka hasil cipher text adalah "(;5G3dbciS" (tidak termasuk tanda "").

Proses dekripsi menggunakan rumus (6) dan (7). Karena karakter "C" memiliki indeks ASCII 8, yang mana adalah kurang dari kunci, maka perhitungannya  $P = (8+94-50) \text{ mod } 94 = 52$ , yaitu karakter "T". Sedangkan untuk karakter ketujuh "d" nilai indeksnya adalah 68, lebih dari kunci, sehingga perhitungannya  $P = (68-50) \text{ mod } 94 = 18$  yaitu "2". Hasil dekripsi adalah "Tugas\_2017!." (tidak termasuk ""). Tabel 1 menunjukkan perhitungan lengkap proses enkripsi dan dekripsi algoritma Caesar cipher yang digunakan.

Tabel 1  
Perhitungan Enkripsi dan dekripsi Caesar Cipher

P	indeks	Enkripsi	C	Dekripsi	P
T	52	$C = (52+50) \text{ mod } 94 = 8$	(	$P = (8+94-50) \text{ mod } 94 = 52$	T
u	85	$C = (85+50) \text{ mod } 94 = 41$	I	$P = (41+94-50) \text{ mod } 94 = 85$	u
g	71	$C = (71+50) \text{ mod } 94 = 27$	;	$P = (27+94-50) \text{ mod } 94 = 71$	g
a	65	$C = (65+50) \text{ mod } 94 = 21$	5	$P = (21+94-50) \text{ mod } 94 = 65$	a
s	83	$C = (83+50) \text{ mod } 94 = 39$	G	$P = (39+94-50) \text{ mod } 94 = 83$	s
_	63	$C = (63+50) \text{ mod } 94 = 19$	3	$P = (19+94-50) \text{ mod } 94 = 63$	_
2	18	$C = (18+50) \text{ mod } 94 = 68$	d	$P = (68-50) \text{ mod } 94 = 18$	2
0	16	$C = (16+50) \text{ mod } 94 = 66$	b	$P = (66-50) \text{ mod } 94 = 16$	0
1	17	$C = (17+50) \text{ mod } 94 = 67$	c	$P = (67-50) \text{ mod } 94 = 17$	1
7	23	$C = (23+50) \text{ mod } 94 = 73$	i	$P = (73-50) \text{ mod } 94 = 23$	7
!	1	$C = (1+50) \text{ mod } 94 = 51$	S	$P = (51-50) \text{ mod } 94 = 1$	!
.	14	$C = (14+50) \text{ mod } 94 = 64$	`	$P = (64-50) \text{ mod } 94 = 14$	.

Tabel Vigenere juga dilakukan modifikasi yaitu menggunakan 94 karakter sehingga tabel memiliki 94 baris dan 94 kolom. Rumus enkripsi dan dekripsi Vigenere cipher yang digunakan adalah sebagai berikut :

$$C = (P_i + K_i) \text{ mod } 94 \tag{8}$$

$$P = (C_i - K_i) \text{ mod } 94 \tag{9}$$

Seperti halnya pada Caesar cipher, rumus dekripsi pada Vigenere cipher juga dilakukan modifikasi pada saat indeks cipher lebih kecil dari kunci ( $C_i < K_i$ ) yaitu

$$P = (C_i + 94 - K_i) \text{ mod } 94 \tag{10}$$

Contoh penerapan Vigenere cipher adalah sebagai berikut :  
Plain text : "Tugas\_2017!." (karakter "" tidak termasuk yang dienkripsi)

kunci : "Imam1@?." (tidak termasuk ""). Hasil enkripsi dan dekripsi dapat dilihat pada tabel 2.

Tabel 2  
Perhitungan Enkripsi dan dekripsi Vigenere Cipher

P	indeks	Enkripsi	C	Dekripsi	P
T	I = 41	$C = (52+41) \bmod 94 = 93$	}	$P = (93-41) \bmod 94 = 52$	T
u	m = 77	$C = (85+77) \bmod 94 = 68$	d	$P = (68+94-77) \bmod 94 = 85$	u
g	a = 65	$C = (71+65) \bmod 94 = 42$	J	$P = (42+94-65) \bmod 94 = 71$	g
a	m = 77	$C = (65+77) \bmod 94 = 48$	P	$P = (48+94-77) \bmod 94 = 65$	a
s	l = 17	$C = (83+17) \bmod 94 = 6$	&	$P = (6+94-17) \bmod 94 = 83$	s
_	@ = 32	$C = (63+32) \bmod 94 = 1$	!	$P = (1+94-17) \bmod 94 = 63$	_
2	? = 31	$C = (18+31) \bmod 94 = 49$	Q	$P = (49-31) \bmod 94 = 18$	2
0	I = 41	$C = (16+41) \bmod 94 = 57$	Y	$P = (57-41) \bmod 94 = 16$	0
1	m = 77	$C = (17+77) \bmod 94 = 0$	Sp	$P = (0+94-77) \bmod 94 = 17$	1
7	a = 65	$C = (23+65) \bmod 94 = 88$	x	$P = (88-65) \bmod 94 = 23$	7
!	m = 77	$C = (1+77) \bmod 94 = 78$	n	$P = (78-77) \bmod 94 = 1$	!
.	l = 17	$C = (14+17) \bmod 94 = 31$	?	$P = (31-17) \bmod 94 = 14$	.

Pada penelitian ini dilakukan penggabungan algoritma Caesar cipher dan Vigenere dengan langkah-langkah enkripsinya adalah sebagai berikut :

1. Sediakan *Plaintext* yang akan dienkripsi.  
*Plaintext* : Imam\_2018

2. Tentukan nilai kunci *Caesar* dan *Vigenere*.  
Kunci *caesar* : 35  
Kunci *vigenere* : Skripsi
3. Konversi *plaintext* dan kunci *Vigenere* ke desimal

Tabel 3.  
Konveris *plaintext* ke desimal

<i>Plaintext</i>	I	m	a	m	_	2	0	1	8
Desimal	41	77	65	77	63	18	16	17	24

Tabel 4.  
Konveris Kunci *Vigenere* ke desimal

Kunci <i>Vigenere</i>	S	k	R	i	p	S	I
Desimal	51	75	82	73	80	83	73

4. Lakukan proses enkripsi *Caesar* yang ditunjukkan oleh tabel 5. Dimana hasil Enkripsi *Caesar* yaitu : l2&2\$UST[
5. Lakukan proses enkripsi *Vigenere* dan konversi ke *Ciphertext*. Pada proses enkripsi *vigenere* ini *plaintext* yang dipakai yaitu hasil dari enkripsi *caesar*. Hasilnya dapat dilihat pada tabel 6. Hasil *Ciphertext* akhir setelah dilakukan Enkripsi *Caesar* dan *Vigenere* yaitu : A }x{tJ>)H

Tabel 5.  
Enkripsi *Caesar*

P	Enkripsi	C
I = 41	$(41 + 35) \bmod 94 = 76$	l
m = 77	$(77 + 35) \bmod 94 = 18$	2
a = 65	$(65 + 35) \bmod 94 = 6$	&
m = 77	$(77 + 35) \bmod 94 = 18$	2
_ = 63	$(63 + 35) \bmod 94 = 4$	\$
2 = 18	$(18 + 35) \bmod 94 = 53$	U
0 = 16	$(16 + 35) \bmod 94 = 51$	S
1 = 17	$(17 + 35) \bmod 94 = 52$	T
8 = 24	$(24 + 35) \bmod 94 = 59$	[

Tabel 6.  
Enkripsi *Vigenere*

No	P	Enkripsi	C
1	l = 76	$(76 + 51) \bmod 94 = 33$	A
2	2 = 18	$(18 + 75) \bmod 94 = 93$	}
3	& = 6	$(6 + 82) \bmod 94 = 88$	x
4	2 = 18	$(18 + 73) \bmod 94 = 91$	{
5	\$ = 4	$(4 + 80) \bmod 94 = 84$	t
6	U = 53	$(53 + 83) \bmod 94 = 42$	J
7	S = 51	$(51 + 73) \bmod 94 = 30$	>
8	T = 52	$(52 + 51) \bmod 94 = 9$	)
9	] = 59	$(59 + 75) \bmod 94 = 40$	H

Langkah-langkah dekripsi penggabungan Caesar cipher dan *Vigenere* cipher adalah sebagai berikut :

1. Sediakan *Ciphertext* yang akan didekripsi.  
*Ciphertext* : A } x { t J > ) H
2. Tentukan nilai kunci *Caesar* dan *Vigenere*.  
Kunci *caesar* : 35  
Kunci *vigenere* : Skripsi
3. Konversi *ciphertext* dan kunci *Vigenere* ke decimal.

Tabel 7.  
Konversis *ciphertext* ke desimal

P	A	}	x	{	t	J	>	)	H
Desimal	33	93	88	91	84	42	30	9	40

4. Lakukan proses dekripsi *Vigenere* yang dapat dilihat pada tabel 8. Hasil Dekripsi *Vigenere* yaitu : l2&2\$UST[

Tabel 8.  
Dekripsi *Vigenere*

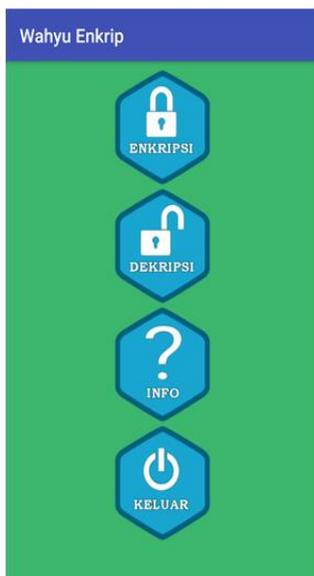
C	Dekripsi	P
A = 33	$(33 + 94 - 51) \bmod 94 = 76$	l
} = 93	$(73 - 75) \bmod 94 = 18$	2
x = 88	$(88 - 82) \bmod 94 = 6$	&
{ = 91	$(91 - 73) \bmod 94 = 18$	2
t = 84	$(84 - 80) \bmod 94 = 4$	\$
J = 42	$(42 + 94 - 83) \bmod 94 = 53$	U
> = 30	$(30 + 94 - 73) \bmod 94 = 51$	S
) = 9	$(9 + 94 - 51) \bmod 94 = 52$	T
H = 40	$(40 + 94 - 75) \bmod 94 = 59$	[

5. Lakukan proses dekripsi *caesar* dan konversi ke *plaintext*. Pada proses dekripsi *caesar* ini *ciphertext* yang dipakai yaitu hasil dari denkripsi *vigenere*. Perhitungannya dapat dilihat pada tabel 9. Hasil *Plaint ext* akhir setelah dilakukan Dekripsi *Vigenere* dan *Caesar* yaitu : Imam\_2018

Tabel 9.  
Deskripsi Caesar

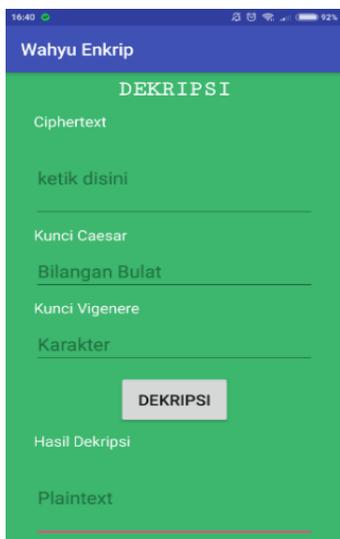
C	Dekripsi	
l = 76	$(76 - 35) \bmod 94 = 41$	I
2 = 18	$(18 + 94 - 35) \bmod 94 = 77$	m
& = 6	$(6 + 94 - 35) \bmod 94 = 65$	a
2 = 18	$(18 + 94 - 35) \bmod 94 = 77$	m
\$ = 4	$(4 + 94 - 35) \bmod 94 = 63$	_
U = 53	$(53 - 35) \bmod 94 = 18$	2
S = 51	$(51 - 35) \bmod 94 = 16$	0
T = 52	$(52 - 35) \bmod 94 = 17$	1
[ = 59	$(59 - 35) \bmod 94 = 24$	8

Metode yang telah dipaparkan sebelumnya diimplementasikan dengan menggunakan bahasa pemrograman *Java* dan dengan aplikasi *Android Studio* dalam pembuatannya. Tampilan yang terdapat dalam aplikasi terdiri dari tampilan menu utama, tampilan enkripsi dan tampilan dekripsi. Pada Tampilan menu utama user dapat memilih kegiatan apa yang ingin dilakukan. Tampilan menu utama dapat dilihat pada gambar 2.



Gambar 2. Tampilan Menu Utama

Pada tampilan Enkripsi pengguna dapat melakukan enkripsi terhadap informasi yang dimiliki. Sedangkan pada tampilan Dekripsi pengguna dapat melakukan dekripsi terhadap *ciphertext* yang dimiliki. Tampilan Enkripsi dapat dilihat pada gambar 3 dan tampilan Dekripsi pada gambar 4.



Gambar 3. Tampilan Enkripsi



Gambar 4. Tampilan Dekripsi

### HASIL DAN PEMBAHASAN

Pengujian dilakukan dengan 4 tipe teks yang berbeda, dengan nilai kunci *caesar* dan kunci *vigenere* yang berbeda-beda. Teks Uji dapat dilihat pada tabel 10.

Tabel 10  
Teks Uji

No.	Kasus Uji
1	Nama Caesar diambil dari Julius Caesar, jenderal, konsul, dan diktator Romawi yang menggunakan sandi ini untuk berkomunikasi dengan para panglimanya.
2	Enkripsi Caesar Secara matematis dituliskan dengan : $C=(P+K)\text{mod}26$ Dengan $C$ =Enkripsi, $P$ =plaintext, dan $K$ =Kunci.
3	GIOVAN BATISTA BELASO MENJELASKAN METODE VIGENÈRE DALAM BUKU LA CIFRA DEL. SIG. GIOVAN BATISTA BELASO (1553);
4	Karakter pengujian : §~↑→JK@ △Çî &*?μΦΩε≥÷√. hasilnya harus sama.

Pengujian dilakukan dengan berbagai teks dan kunci yang berbeda dimaksudkan agar dapat mengetahui apakah metode yang diusulkan mampu melakukan enkripsi dan dekripsi dengan tepat untuk teks dan kunci apapun. Hasilnya dapat dilihat di tabel 11.

Tabel 11.  
Hasil Pengujian

Teks	Kunci Caesar	Kunci Vigenere	Enkripsi (Ciphertext)	Dekripsi (Plaintext)	Hasil
Ke-1	9	A1@	x{8-!-!>-.10%.9 48/- .4Jd@8% @?;!>-.UJ&0: 0>{7V:6;*>A(UJ ,;:/5'- 0>:;);C%IE{93:81*2319 -';>- */5:4:% IA?*A'I.!=7+8A*4 7{>5:/1*2-*I<{-;:- *28% 8-*D-H	Nama Caesar diambil dari Julius Caesar, jenderal, konsul, dan diktator Romawi yang menggunakan sandi ini untuk berkomunikasi dengan para panglimanya.	<b>Sukses</b>
Ke-2	352	Vigenere	cA<AA?O8>t24K0NMq8 40J0Z<!G6<9CEB>7:CM; EB+4?M<4J6!AOgVpwU n\zVE>@_TQs4F6==>tr F:N80F:YV}w?,4:=L4TCJ Q50FM'jH?2A[	Enkripsi Caesar Secara matematis dituliskan dengan : $C=(P+K)\text{mod}26$ Dengan C=Enkripsi, P=plaintext, dan K=Kunci.	<b>Sukses</b>
Ke-3	29	Tugas akhir	:jUVSk LH\ZFhG TbLKZW1@YTJWiA]RI _qaKTaaE*]QX8bXE2aA VHU15iQU2iA*JQWEU &DWi.*ZQX!4MIasAX'J RG]YTS=BOSIdB4.1GR3 3B	GIOVAN BATISTA BELASO MENJELASKAN METODE VIGENÈRE DALAM BUKU LA CIFRA DEL. SIG. GIOVAN BATISTA BELASO (1553);	<b>Sukses</b>
Ke-4	105	Chara	;V`YdZ` }^UcUtXYV\}(n ?9?lnyv>zn]OrW\cg`IXV` tanhOIO	Karakter pengujian : JK@ &*?. hasilnya harus sama.	<b>Gagal</b>

Dari hasil pengujian algoritma dengan 4 tipe teks dan kunci yang berbeda-beda yang sudah dilakukan maka dapat diketahui bahwa algoritma penggabungan antara *caesar cipher* dan *vigenere cipher* secara umum dapat melakukan enkripsi dan dekripsi. Namun pada percobaan dengan Teks uji ke-4 didapatkan hasil gagal karena teks uji yang dipakai berada diluar batasan dari algoritma yang diusulkan. Tingkat kesuksesan algoritma ini adalah 0.75 atau 75%.

**SIMPULAN**

Dapat disimpulkan bahwa, algoritma yang diusulkan yaitu penggabungan antara *caesar cipher* dan *vigenere cipher* secara umum dapat melakukan enkripsi dan dekripsi dengan tingkat kesuksesan 75%. Hasil enkripsi dan dekripsi akan tepat terutama jika *plain text* maupun *cipher text*

yang digunakan berada dalam batasan karakter yang digunakan.

Ketepatan enkripsi dan dekripsi ini berlaku pada semua tipe teks dengan kunci yang berbeda-beda, namun jika pada teks terdapat karakter yang berada di luar batasan karakter yang digunakan maka karakter tersebut tidak dapat diproses. Karakter yang dipakai yaitu ASCII dengan nomor index antara 32 sampai 125 (total 94). Maka dari itu, yang perlu diperhatikan adalah pemakaian karakter dan kunci yang tepat agar proses enkripsi dan dekripsi dapat berjalan dengan optimal.

**DAFTAR PUSTAKA**

Kusumawardani, C. (2010). Implementasi Steganogrfi Dengan Penggabungan Kriptografi Metode Vinegere Dan

- Caesar Substitution. *Jurnal Informatika*.
- Latifah, R., Ambo, S. N., & Kurnia, S. I. (2017). MODIFIKASI ALGORITMA CAESAR CHIPER DAN RAIL FENCE UNTUK PENINGKATAN KEAMANAN TEKS ALFANUMERIK DAN KARAKTER KHUSUS. *Seminar Nasional Sains dan Teknologi*. Jakarta: Universitas Muhammadiyah Jakarta.
- Nasution, S. D., Ginting, G. L., Syahrizal, M., & Rahim, R. (2017). Data Security Using Vigenere Cipher and Goldbach Codes Algorithm. *International Journal of Engineering Research & Technology (IJERT)*, 360-363.
- Prayitno, A., & Nurdin, N. (2017). ANALISA DAN IMPLEMENTASI KRIPTOGRAFI PADA PESAN RAHASIA MENGGUNAKAN ALGORITMA CIPHER TRANSPOSITION. *JESIK Jurnal Elektronik Sistem Informasi dan Komputer*, 1-11.
- Rahim, R. (2016). PENYISIPAN PESAN DENGAN ALGORITMA PIXEL VALUE DIFFERENCING DENGAN ALGORITMA CAESAR CIPHER PADA PROSES STEGANOGRAFI. *Jurnal TIMES*, 6-11.
- Saputra, I., Hasibuan, N. A., Mesran, M., & Rahim, R. (2017). Vigenere Cipher Algorithm with Grayscale Image Key Generator for Secure Text File. *International Journal of Engineering Research & Technology (IJERT)*, 266-269.
- 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)*.
- Setyaningsih, E. (2015). *Kriptografi & Implementasinya Menggunakan Matlab*. Yogyakarta: Penerbit Andi.