Metode*Hybrid* dan *Riverst Shamir Adleman* Menggunakan Algoritma Kriptografi *Klasik Vigenere*

Mursid
mursidjpr73@gmail.com

Staf Pengajar pada Program Studi Teknik Informatika
Fakultas Ilmu Komputer dan Manajemen
Universitas Sains dan Teknologi Jayapura

Abstraksi *- Menjaga kemananan pesan sudah merupakan hal yang sangat penting baik dalam suatu organisasi maupun pribadi terutama di zaman teknologi dan informasi saat ini. Agar pesan yang dikirim tidak jatuh ke tangan orang-orang yang tidak berkepentingan, maka dibuatkan penyandian untuk menjaga kerahasiaan suatu pesan tetap aman. Dengan metode kriptografi klasik menggunakan Vigenere Chiper dengan RSA (Riverst Shamir Adleman) merupakan salah satu metode pengamanan pesan yang akandigunakan.Dalam hal ini proses yang pertama dilakukan adalah melakukan enkripsi pada vigenere chiperyang menghasilkan suatu chiperteks sementara. Kemudian hasil chiperteks sementara menjadi plainteks padaAlgoritma RSA dan selanjutnyadienkripsilagi sehingga menghasilkan suatuchipertext yang sesungguhnya. Penggabungan dua metode ini menghasilkansuatu chipertext yang lebih kuat dan sulit untuk di pecahkan.*

Kata kunci: Kriptogtafi, Enkripsi, Dekripsi, RSA, Vigenere Chiper

1. PENDAHULUAN

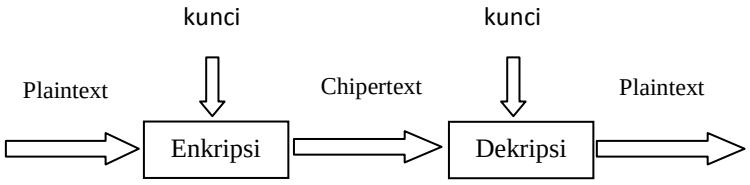
Keamanan sistem komunikasi menjadi syarat yang harus dipenuhi oleh semua pihak yang terlibat di dalam sistem tersebut. Pertukaran pesan atau informasi membutuhkan tingkat keamanan yang tinggi, karena pengamanan pesan atau informasi berfungsi melindungi pesan atau informasi agar tidak dapat dibaca oleh kriptanalisis, serta mencegah kriptanalisis memodifikasi pesan atau informasi. Sejak dahulu teknik kriptografi dipercaya untuk menangani masalah keamanan pesan atau informasi[1].

Dengan semakin berkembangnya teknologi komputer, sistem *multiuser* sudah sangatmemungkinkan dimana suatu data dapat dibagikan kepada komputer atau user lain dalam suatujaringan komputer ataupun jaringan yang lebih luas lagi yaitu internet. Tetapi ada data yangmemerlukan *privacy* dan harus dijaga kerahasiannya. Data-data penting ini harus dijaga dari pihakpihakyang tidak bertanggung jawab baik terhadap pemalsuan, pencurian maupun pengubahan datasecara illegal[2].

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*Cryptography is the art and science of keeping messages secure*). Kata “seni” di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut mungkin berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia mempunyai nilai estetika tersendiri. Istilah-istilah yang digunakan dalam bidang kriptografi:

1. **Plaintext** (*P*) adalah pesan yang hendak dikirimkan (berisi data asli).
2. **Chipertext** (*C*) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
3. **Enkripsi** (fungsi E) adalah proses pengubahan *plaintext* menjadi *chipertext*.
4. **Dekripsi** (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *chipertext* menjadi *plaintext*,sehingga berupa data awal/asli.
5. **Kunci** adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yangtelah dijelaskan di atas, proses enkripsi mengubah *plaintext* menjadi *chipertext* (dengan menggunakan kuncitertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti. Untuk melihat ilustrasi dari proses kriptografi dapat dilihat pada gambar 1, mekanisme kriptografi[3].



Gambar 1. Mekanisme kriptografi

2. TINJAUAN PUSTAKAN

a. Vigenere Chiper

Metode *Vigenere chiper* merupakan bagian darikriptografi klasik. Nama *Vigenere* diambil dari seorang yang bernama *Blaise de Vigenere*. *Vigenere cipher* merupakan contoh *chiper* alfabet-majemuk "manual" yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenere pada abad 16, meskipun Giovan Batista Belaso telah menggambarkannya pertama kali pada tahun 1553 seperti ditulis di dalam bukunya *La Cifra del Sig,* tetapi algoritma ini baru dikenal luas 200 tahun kemudian yang oleh penemunya tersebut kemudian dinamakan *Vigenere chiper. Chiper* ini berhasil dipecahkan oleh Babage dan Kasiski pada pertengahan abad ke-19.Metode *Vigenere chiper* sangat dikenal karena di samping menggunakan rumus matematika, *chiper*menggunakan persegi *Vigenere* untuk melakukan enkripsi maupun dekripsi.Persegi vigenere digunakan untuk memperoleh*chiperteks* dengan menggunakan kunci yang sudah ditentukan (Tabel 1).Jika panjang kunci lebih pendek daripanjang plainteks maka kunci diulang penggunaannya(sistem periodik).Enkripsi dengan metode *Vigenere chipher*, menggunakan persegi *Vigenere* dengan cara tarik garis vertikal dari huruf plainteks ke bawah, lalu tarik garis horizontal ke huruf kunci kekanan.Perpotongan kedua garis tersebut menyatakan huruf chiperteksnya. Dekripsi pada *Vigenere chiper*dilakukan dengan cara yang berkebalikan, yaitu menarik garis horizontal dari huruf kunci sampai kehuruf chiperteks yang dituju, lalu dari huruf chiperteks tarik garis vertikal sampai ke huruf plainteks. Secara matematis, misalkan kunci sepanjang ***i*** adalah rangkaian$\mathbf{K_1, K_2, ..., K_i}$, plainteks adalah rangkaian $\mathbf{P_1,P_2 ..., P_i}$, dan chiperteks adalah rangkaian $\mathbf{C_1C_2 ... C_i}$, sehingga enkripsi pada *Vigenere chiper* dapat dinyatakan:

$$C_i = (P_i + K_i) \; mod \; 26 \qquad (1)$$

Secara matematis dekripsi dinyatakan dengan cara mengubah Persamaan (1),yang dapat dinyatakan dengan memindah ruaskan sehingga diperoleh persamaan:

$P_i = (C_i - K_i) \; mod \; 26$, jika$C_i >= K_i$

atau

$$P_i = (C_i + 26 - K_i) \; mod \; 26, \text{ jika } C_i <= K_i \qquad (2)$$

Keterangan:

C_i = nilai desimal karakter chipertext ke-i,

P_i = nilai desimal karakter plaintext ke-i,

K_i = nilai desimal karakter kunci ke-i

Tabel 1. Tabel Bujur Sangkar Vigenere

		Plaintext																								
		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
kunci	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
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Kelemahan dari Algoritma Vigenere Cipher yaitu jika panjang kunci yang digunakan kurang dari panjang plainteks. Kurang panjangnya kunci terhadap plainteks menyebabkan kunci akan diulang hingga panjang kunci tersebut sama dengan panjang plainteks. Hal ini menyebabkan kemungkinAN timbulnya perulangan string pada chiperteks hasil enkripsi yang dapat dimanfaatkan untuk menemukan panjang kunci dan lebih lanjut dimanfaatkan untuk memecahkan chiperteks tersebut. Orang yang pertama berhasil menemukan kelemahan vigenere chiper dan memecahkan chiperteksnya adalah Friedreich Kasiski pada tahun 1863 yang disebut metode Kasiski[4].

Kelebihan dari Algoritma Vigenere Chiper adalah cara kerjanya mudah dimengerti dan dijalankan. Karakteristik dari chiper adalah setiap huruf chiperteksnya dapat memiliki kemungkinan banyak huruf plainteks.

b. RSA (Rivest, Shamir, Adleman)

RSA merupakan algoritma kriptografi asimetris. Ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman. Nama RSA sendiri diambil dari inisial nama depan ketiga penemunya tersebut. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci public dan kunci pribadi. Kunci public boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci pribadi hanya pihak–pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi.

Keamanan sandi RSA terletak pada sulitnya memfaktorkan bilangan yang besar. Sampai saat ini RSA masih dipercaya dan digunakan secara luas di internet. (*Kriptografi Kunci Publik: Sandi RSA*, 2008).

Skema algoritma kunci publik Sandi RSA terdiri dari 3 (tiga) proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi.

Sebelumnya diberikan terlebih dahulu beberapa konsep perhitungan matematis yang digunakan RSA (*RSA and Public KeyCriptography*, 2003, hlm 61).

C = M^e mod n (fungsienkripsi)

M = C^d mod n (fungsidekripsi)

Keterangan:

C = Chiperteks

M = Message / Plainteks

e = kuncipublik

d = kunciprivat

n = modulo pembagi

Kedua pihak harus mengetahui nilai **e** dan nilai **n** ini, dan salah satu pihak harus memiliki **d** untuk melakukan dekripsi terhadap hasil enkripsi dengan menggunakan *public key* **e**.

c. Algoritma Pembentukan Kunci:

1. Tentukan *p* dan *q* bernilai dua bilangan Prima besar, acak dan dirahasiakan.$p \neq q$, *p* dan *q* memiliki ukuran sama.
2. Hitung $n = pq$. Dan hitung $\varphi(n) = (p-1)(q-1)$. Bilangan *integer n* disebut (*RSA*) *modulus*.
3. Tentukan *e* bilangan Prima acak, yang memiliki syarat:$1 < e < \varphi(n)$
   GCD(*e*, φ(*n*)) = 1, disebut *e* relatif prima terhadap φ(*n*), Bilangan integer *e* disebut (*RSA*) *enciphering exponent*.
4. Memakai algoritma Euclid yang diperluas (*Extended Eucledian Algorithm*).
   Menghitung bilangan khusus *d*,

   syarat $1 < d < \varphi(n)$
   $d \equiv e^{-1} \bmod \varphi(n)$
   $ed \equiv 1 \pmod{\varphi(n)}$
   $ed \equiv 1 + k.\varphi(n)$ untuknilai k integer.

   Bilangan integer *d* disebut (*RSA*) *deciphering exponent*.

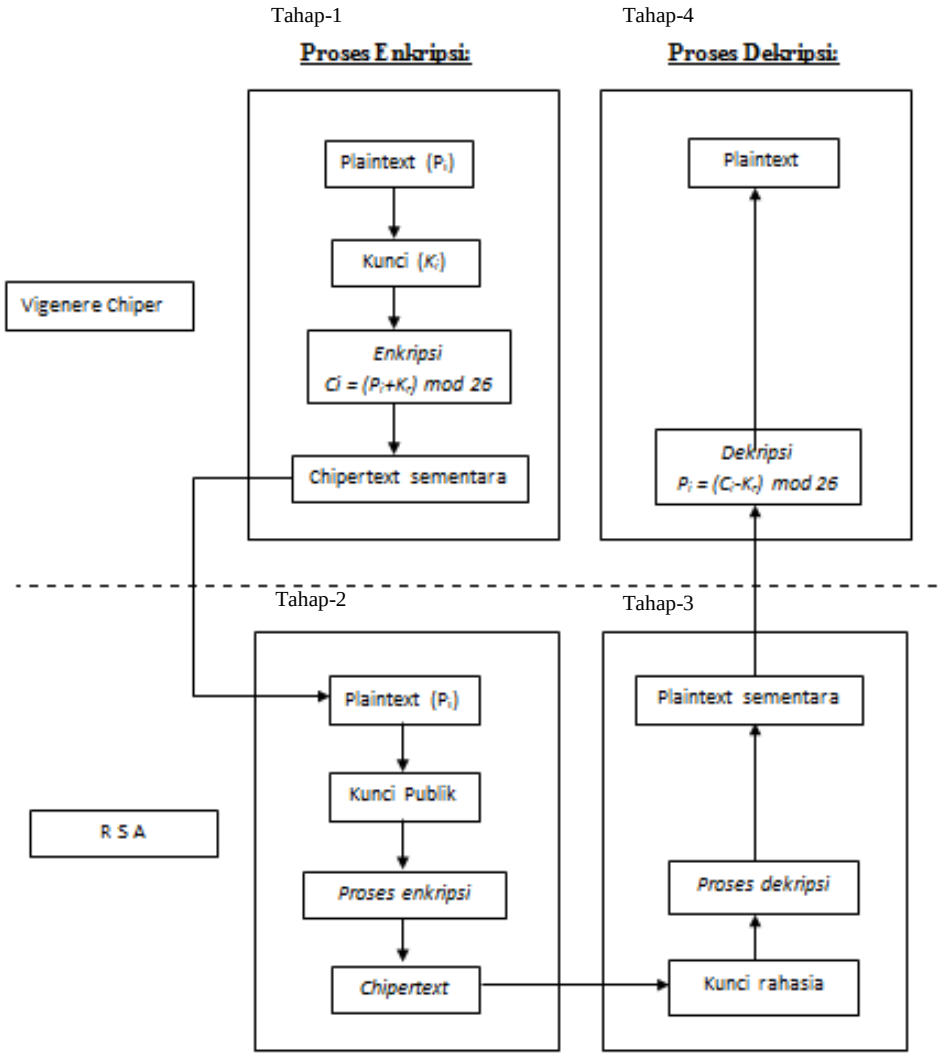
5. Nilai (*n*,*e*) adalah nilai yang boleh dipublikasi.

   Nilai *d*, *p*, *q*,φ(*n*) adalah nilai yang harus dirahasiakan.

   Pasangan (*n*,*e*) merupakan kunci publik.
   Pasangan (*n*,*d*) merupakan kunci rahasia.

3. HASIL PROSES ENKRIPSI DAN DEKRIPSI

Proses enkripsi dan deskripsi menggunakan *vigenere chiper* yang diperkuat dengan RSA, dilakukan dalam empat tahap seperti pada (gambar 2).



Gambar 2. Alur proses enkripsi dan dekripsi menggunakan Vigenere Chiper dan RSA

a. **Proses Enkripsi Pertama dengan Metode Vigenere Chiper**

Plaintext: KEAMANAN KOMPUTER

Kunci: pasca

Dari Plaintext dengan kata kunci di atas diperoleh:

Plaintext	K	E	A	M	A	N	A	N	K	O	M	P	U	T	E	R
Kunci	p	a	s	c	a	p	a	s	c	a	p	a	s	c	a	p
Chipertext 1	Z	E	S	O	A	C	A	F	M	O	B	P	M	V	A	G
Nilai	25	4	18	14	0	25	0	5	11	14	1	15	12	21	4	6

Penyelesaian I:

Pada contoh diatas kata kunci **PASCA** diulang secara periodik hingga panjang kunci sama dengan panjang plainteksnya. Jika dihitung dengan rumus enkripsi vigenere, plainteks huruf pertama **K** (yang memiliki nilai **Pi=10**) akan dilakukan pergeseran dengan huruf **P** (yang memiliki **Ki=15**) maka prosesnya sebagai berikut:

C_i = (P_i + K_i) mod 26

= (10 + 15) mod 26

= 25 mod 26

= 25

C_i=25, maka huruf chipertext dengan nilai **25** adalah **Z.** Begitu seterusnya dilakukan pergeseran sesuai dengan kunci pada setiap huruf hingga semua plainteks telah terenkripsi menjadi chipertext. Setelah semua huruf terenkripsi, maka proses dekripsinya dapat dihitung sebagai berikut:

P_i = (C_i – K_i) mod 26

= (25 – 15) mod 26

= 10 mod 26

= 10

P_i= 10 maka huruf plainteks dengan nilai **10** adalah **K**. Begitu seterusnya dilakukan pergeseran sesuai dengan kunci pada setiap huruf hingga semua chipertext telah terdekripsi menjadi plainteks.

Penyelesaian II:

Plainteks huruf pertama **N** (yang memiliki nilai **Pi=13**) akan dilakukan pergeseran dengan huruf **S** (yang memiliki **Ki=18**) maka prosesnya sebagai berikut:

C_i = (P_i + K_i) mod 26

= (13 + 18) mod 26

= 31 mod 26

= 5 *// sisa hasil bagi dari 31 mod 26 adalah 5*

C_i=5, maka huruf chipertext dengan nilai **5** adalah **F.** Begitu seterusnya dilakukan pergeseran sesuai dengan kunci pada setiap huruf hingga semua plainteks telah terenkripsi menjadi chipertext.Setelah semua huruf terenkripsi, maka proses dekripsinya dapat dihitung sebagai berikut:

P_i = (C_i – K_i) mod 26

= (5 – 18) + 26

= - 13 + 26*//* dijumlahkandengan 26 karenaC_i<= K_i

= 13

P_i=13 maka huruf plainteks dengan nilai **13** adalah **N**. Begitu seterusnya dilakukan pergeseran sesuai dengan kunci pada setiap huruf hingga semua chipertext telah terdekripsi menjadi plainteks.

b. Proses Enkripsi Kedua dengan Metode RSA

Terlebih dahulu mencari kunci publik dan kunci private dengan mengambil dua buah bilangan prima sembarang.
Misalkan: p = 31; q = 37

1. N = p.q = (31)(37) = 1147

   φ(N) = (p – 1)(q – 1) = (31-1)(37-1) = (30)(36) = 1080

2. Menentukan Public key: e<1080, e>1

   - e=13
   - ed=1 (mod ϕ(N))
     13d=1 mod 1080

   Gunakan algoritma Euclid yang diperluas untuk mendapatkan d:

k	0	1	2	3
r_k	1080	13	1	0

q_k		83	13	
s_k	1	0	1	
t_k	0	1	-83	

Berdasarkan Theorema "Jika $0 \leq k \leq n + 1$, maka $r_k = s_k a + t_k b$" :

(1)(1080)+(-83)(13) = 1 mod 1080
(-83)(13) = 1 mod 1080
d=-83 atau 997

- Maka,

  Public Key = (e,N)=(13, 1147)
  Private Key = (d,N)=(997, 1147)

3. Chiperteks 1 dari hasil enkripsi Vigenere (m) = ZESOACAFMOBPMVAG

Chiperteks 1	Z	E	S	O	A	C	A	F	M	O	B	P	M	V	A	G
Kode Ascii	90	69	83	79	65	67	65	70	77	79	66	80	77	86	65	71

m dipecah menjadi sebelas blok yang berukuran 3 digit:
$m_1 = 906$, $m_2 = 983$, $m_3 = 796$, $m_4 = 567$ $m_5 = 657$ $m_6 = 077$
$m_7 = 796$ $m_8 = 680$ $m_9 = 778 m_{10} = 665$ $m_{11} = 71$

Enkripsi menggunakan Public Key (e,N) = (13 , 1147)

$c = m^e \bmod N$

$c_1 = m_1^e \bmod N = 906^{13} \bmod 1147 = 143$
$c_2 = m_2^e \bmod N = 983^{13} \bmod 1147 = 509$
$c_3 = m_3^e \bmod N = 796^{13} \bmod 1147 = 301$
$c_4 = m_4^e \bmod N = 567^{13} \bmod 1147 = 793$
$c_5 = m_5^e \bmod N = 657^{13} \bmod 1147 = 99$
$c_6 = m_6^e \bmod N = 077^{13} \bmod 1147 = 585$
$c_7 = m_7^e \bmod N = 796^{13} \bmod 1147 = 301$
$c_8 = m_8^e \bmod N = 680^{13} \bmod 1147 = 643$
$c_9 = m_9^e \bmod N = 778^{13} \bmod 1147 = 334$
$c_{10} = m_{10}^e \bmod N = 665^{13} \bmod 1147 = 369$
$c_{11} = m_8^e \bmod N = 71^{13} \bmod 1147 = 266$

jadi, Chiperteks akhir yang dihasilkan adalah:

c = 143 509 301 793 99 585 301 643 334 369 266

Kode Ascii	**14**	**35**	**09**	**30**	**17**	**93**	**99**	**58**	**53**	**01**	**64**	**33**	**34**	**36**	**92**	**66**
Chiperteks 2	**<SO>**	**#**	**<TAB>**	**<RS>**	**<DC1>**	**]**	**c**	**:**	**5**	**<SOH>**	**@**	**!**	**“**	**$**	****	**B**

c. Proses Dekripsi Pertama dengan Metode RSA

Pesan chiperteks 2 dalam kode ASCII : 143 509 301 793 99 585 301 643 334 369 266
Private Key = (d,N) = (997 , 1147)
$m = c^d \bmod N$
$m_1 = c_1^d \bmod N = 143^{997}$
mod 1147 = 906
$m_2 = c_2^d \bmod N = 509^{997} \bmod 1147 = 983$

$m_3 = c_3^d \bmod N = 301^{997} \bmod 1147 = 796$
$m_4 = c_4^d \bmod N = 793^{997} \bmod 1147 = 567$
$m_5 = c_5^d \bmod N = 99^{997} \bmod 1147 = 657$
$m_6 = c_6^d \bmod N = 585^{997} \bmod 1147 = 077$
$m_7 = c_7^d \bmod N = 301^{997} \bmod 1147 = 796$
$m_8 = c_8^d \bmod N = 643^{997} \bmod 1147 = 680$
$m_9 = c_9^d \bmod N = 334^{997} \bmod 1147 = 778$
$m_{10} = c_{10}^d \bmod N = 369^{997} \bmod 1147 = 665$
$m_{11} = c_{11}^d \bmod N = 266^{997} \bmod 1147 = 71$

Maka diperoleh pesan (plainteks) atau dekripsi pertama yang nantinya akan di dekripsi lagi dengan Vigenere Chiper untuk mendapatkan plainteks yang sebenarnya:

Kode Ascii	90	69	83	79	65	67	65	70	77	79	66	80	77	86	65	71
Chiperteks 2	Z	E	S	O	A	C	A	F	M	O	B	P	M	V	A	G
Kunci	p	a	s	c	a	p	a	s	c	a	p	a	s	c	a	p
Nilai Desimal	10	4	0	12	0	13	0	13	10	14	12	15	20	19	4	17
Plaintext	K	E	A	M	A	N	A	N	K	O	M	P	U	T	E	R

m = 906 983 796 567

657 077 796 680 778 665 71

Kode Ascii	90	69	83	79	65	67	65	70	77	79	66	80	77	86	65	71
Plainteks 1	Z	E	S	O	A	C	A	F	M	O	B	P	M	V	A	G

d. Proses Dekripsi Kedua dengan Metode Vigenere Chiper

Hasil dekripsi dari Metode RSA, selanjutnya didekripsi lagi dengan menggunakan metode Vigenere Chiper.
Penyelesaian:

Pencarian huruf **K**

P_i = (C_i – K_i) mod 26
= (25 – 15) mod 26
= 10 mod 26, **10,** adalah Huruf **K** (Lihat tabel 1)

Pencarian huruf **N**

P_i = (C_i – K_i) mod 26
= (2 – 15) + 26
= -13 + 26
= 13, adalah Huruf **N** (lihat tabel 1),

4. KESIMPULAN

Algoritma Vigenere Chiper dengan kunci lebih pendek dari panjang plainteksnya memberikan peluang untuk dapat dipecahkan. Metode yang digunakan untuk memecahkan chiperteks dari vigenere yaitu dikenal dengan metode Kasiski. RSA dengan dua kunci yaitu *public key* dan *private key* dapat memberikan keamanan pesan yang lebih aman. Dengan menggabungan metode Vigenere Chiper dan RSA menghasilkan chiperteks yang lebih kuat yaitu dengan dua kali proses penyandian (*enkripsi*) dan dua kali proses *dekripsi* sehingga memberikan tingkat keamanan pesan yang lebih lebih aman dan sulit dipecahkan.

5. DAFTAR PUSTAKA

[2] Erna Kumalasari Nurnawati, 2008, *Analisis Kriptografi Menggunakan Algoritma Vigenere Cipher Dengan Mode Operasi Cipher Block Chaining (CBC)*, Seminar Nasional Aplikasi Sains Dan Teknologi.

[1] Juliadi, Bayu Prihandono, Nilamsari Kusumastuti, 2016, *Kriptografi Klasik Dengan Metode Modifikasi Affine Cipher Yang Diperkuat dengan vigenere Cipher,* Volume 02, No. 2 (2013), hal 87– 92.

[5] Mollin, Richard A., 2002, *RSA and Public-Key Cryptography*. Florida, Boca Raton: CRC Press LLC

[3] Putu H. Arjana1, Tri Puji Rahayu , Yakub, Hariyanto, 10 Maret 2012, *Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper,* Yogyakarta.

[4] Riyanto, M. Zaki., &ArdhiArdian, 2008,*KriptografiKunciPublik : Sandi RSA*. http://sandi.math.web.id, diaksespada 13 Februari 2018.