Perancangan Aplikasi Penyandian Pesan Teks Menggunakan Vigenere Chiper Dan Algoritma Elgamal

[1)]Basyiah
STMIK Budi Darma Medan, Jl. Sisingamangaraja No. 388 Simpang Limun Medan
http://stmik-budidarma.ac.id //Email: iah.cuiith@gmail.com

[2)]Fahmy Syahputra
STMIK Budi Darma Medan, Jl. Sisingamangaraja No. 388 Simpang Limun Medan
http://stmik-budidarma.ac.id //Email: fahmysyahputra@gmail.com

ABSTRAK
The development of technology and information, especially in the field of information communication, is very rapidly developing, one of them is the communication media of smart phones. one of the facilities provided by smart phones is the exchange of information in the form of sending text messages through Short Message Service (SMS). This information can be in the form of important data that not all parties can find out. Some risks that can threaten message security in SMS services include SMS Spoofing, Snooping SMS and SMS Interception.
The message security system in the form of text is one of them with a cryptographic system. Cryptography is a message security science that aims to maintain the confidentiality of information contained in data so that information cannot be known by irresponsible parties. Cryptography changes the meaningful writing to be meaningless by using various kinds of cryptographic algorithms. The algorithms used are ElGamal and Vigenere Chiper. The ElGamal algorithm uses 2 different keys in encrypting and decrypting the public key for encryption and the private key for decryption. While Vigenere chipers only use one key that is the same for encryption and description.
With the text message encoding application using the ElGamal and Vigenere Chiper algorithms, it is expected to help smart phone users with the operating system.

Kata Kunci :Penyandian Pesan Teks, Algoritma ElGamal,Vigenere Chiper

PENDAHULUAN

Perkembangan teknologi dan informasi saat ini sangat pesat terutama dibidang informasi komunikasi khusunya di dunia *mobile* seperti telepon seluler yang sudah menjadi bagian dari gaya hidup masyarakat sebagai alat komunikasi. Berkembangnya teknologi telepon genggam dapat dilihat dengan munculnya berbagai macam sistem operasi yang lengkap seperti komputer, diantaranya adalah android.Android adalah sebuah sistem operasi untuk perangkat telepon berbasis *linux* yang mencakup *middleware*, aplikasi dan menyediakan *flatform* terbuka bagi para pengembang untuk menciptakan aplikasi.

Salah satu fasilitas yang disediakan oleh *handphone* android yaitu pertukaran informasi berupa pengiriman pesan teks melalui *Short Message Service* (SMS). Adanya kemungkinan *handphone* digunakan oleh pihak lain baik dengan sengaja maupun tidak sengaja membuat pihak lain dapat membuka dan mengetahui isi dari pesan tersebut. Beberapa resiko yang dapat mengancam keamanan pesan pada layanan SMS antara lain SMS *Spoofing*, SMS *Snooping* dan SMS *Interception*. Dengan adanya beberapa celah keamanan sms maka dibutuhkan sistem penyandian pesan teks yang mampu menjaga kerahasiaan isi pesan tersebut.

Kriptografi adalah ilmu keamanan pesan yang bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak bertanggung jawab.Kriptografi mengubah tulisan yang semula bermakna menjadi tidak bermakna dengan menggunakan berbagai macam algoritma kriptografi [1]. Dalam kriptografi terdapat dua konsep utama yaitu enkripsi dan deskripsi. Enkripsi adalah proses dimana data yang dikirim berupa data jelas yang akan diubah menjadi data yang hampir tidak dapat dikenali, sedangkan deskripsi mengubah kembali data yang tersamarkan menjadi data awal yang dapat dikenali.

Algoritma pada kriptografi klasik beroperasi pada mode karakter sedangkan pada kriptografi modern beroperasi pada mode bit. Salah satu algoritma kriptografi klasik adalah Vigenere Chiper [2]. Kode Vigenere termasuk kode abjad-majemuk

(*polyalphabetic subsitution chiper*). Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenere pada abad 16 tahun 1586. Teknik dari subsitusi Vigenere bisa dilakukan dengan dua cara yaitu angka dan huruf. Salah satu algoritma kriptografi modern adalah algoritma ElGamal. ElGamal adalah suatu *public key* yang dibuat pada tahun 1985. Keamanan dari algoritma ElGamal terletak pada susahnya perhitungan logaritma pada GF(p) ketika p merupakan bilangan prima yang besar. Logaritma ini disebut logaritma diskret karena nilainya berhingga dan bergantung pada bilangan prima yang digunakan. Karena bilangan prima yang digunakan adalah bilangan prima besar, maka sangat sulit bahkan tidak mungkin menurunkan kunci rahasia dari kunci publik yang diketahui walaupun serangan dilakukan dengan menggunakan sumber daya komputer yang sangat besar.

Berdasarkan latar belakang masalah tersebut diperlukan adanya pengidentifikasian pokok-pokok permasalahan yang terjadi, adapun permasalahan yang dimaksud yaitu :

1. Bagaimana cara menyandikan pesan teks *Short Message Service* (SMS) ?
2. Bagaimana cara enkripsi dan deskripsi pesan teks *Short Message Service* (SMS) dengan menggunakan algoritma ElGamal dan Vigenere Chiper?
3. Bagaimana merancang aplikasi penyandian pesan teks SMS berbasis android?

Batasan masalah berfungsi untuk membatasi melebarnya pembahasan permasalahan yang ditemukan. Adapun batasan masalah dalam skripsi ini yaitu :

1. Input berupa pesan teks (sms)
2. Spesifikasi pesan teks (panjang 1 pesan sms) disesuaikan dengan standart teknologi *Global System for Mobile Communication* (GSM)
3. Menggunakan bahasa pemrograman android
4. Aplikasi menggunakan algoritma Vigenere Chiper dan ElGamal
5. Algoritma Vigenere Chiper hanya menyandikan input berupa huruf
6. Algoritma ElGamal menyandikan input berupa huruf, angka dan simbol
7. Panjang kunci pada algoritma Vigenere Chiper harus sama dengan panjang *plaintext*
8. Aplikasi hanya dapat berjalan pada perangkat *mobile* berbasis android
9. Menggunakan android *Ice Cream Sandwich* (4.0.3)
10. Menggunakan emulator *platform* Android SDK sebagai *virtual device*
11. Aplikasi menggunakanADT Eclipse

Adapun tujuan penelitian yang telah di lakukan yaitu :

1. Mengetahui cara menyandikankan pesan teks pada*Short Message Service*
2. Mengetahui cara enkripsi dan deskripsi pesan teks *Short Message Service* (SMS) dengan menggunakan algoritma ElGamal dan Vigenere Chiper
3. Merancang aplikasi penyandian pesan teks berbasis android

Manfaat penelitian yang dilakukan yaitu :

1. Memberikan jaminan kerahasiaan informasi pada pengguna perangkat *mobile* berbasis android dalam pengiriman dan pembacaan pesan teks *Short Message Service* (SMS)
2. Memberikan rasa aman kepada pengirim pesan, karena pesan SMS sudah tersandikan
3. Meminimalisir tindakan para kriptanalis maupun orang-orang yang tidak berhak untuk mendistribusikan data

LANDASAN TEORI

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *cripto* dan *grapish*. *Cripto* berarti *secret* (rahasia) dan *grapish* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain.

2.1.1 Sejarah Kriptografi

Kriptografi sudah digunakan 4000 tahun yang lalu, diperkenalkan oleh orang orang Mesir lewat *hieroglyph*. Dikisahkan pada Zaman Romawi Kuno, Julius Caesar ingin mengirimkan pesan rahasia kepada seorang jenderal di medan perang. Pesan tersebut dikirimkan melalui seorang kurir. Karena pesan tersebut mengandung rahasia, Julius Caesar tidak ingin pesan rahasia tersebut sampai terbuka di jalan. Ia mengacak pesan tersebut hingga menjadi suatu pesan yang tidak dapat dipahami oleh siapapun kecuali oleh jenderalnya saja. Tentu sang jenderal telah diberi tahu sebelumnya bagaimana cara membaca pesan teracak tersebut [8].

Pada Zaman Romawi juga telah ada alat pembuat pesan rahasia yang disebut *Scytale* yang digunakan oleh tentara Sparta [6]. *Scytale* merupakan suatu alat yang memiliki pita panjang dari daun papirus dan ditambah dengan sebatang silinder. Mula-mula pengirim pesan menuliskan pesannya di atas

pita papirus yang digulung pada batang silinder.Setelah itu pita dilepaskan dan dikirim.

2.1.2 Algoritma Kriptografi

Algoritma kriptografi dibagi menjadi tiga berdasarkan kunci yang dipakainya :

1. Algoritma Simetri
   Algoritma ini sering disebut algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan deskripsi. Algoritma yang memakai kunci simetri di antaranya ialah DES, RC2, RC4, RC5, RC6, IDEA, AES dan OTP
2. Algoritma Asimetri
   Sering disebut algoritma kunci publik, dengan arti kunci yang digunakan untuk melakukan enkripsi dan deskripsi berbeda. Pada algoritma asimetri, kunci terbagi menjadi dua, yaitu kunci umum dan kunci rahasia. Contoh algoritma Asimetri adalah DSA, RSA, *Diffie-Hellman* (DH), *Elliptic Curve Cryptography* (ECC), Kriptografi Quantum dan sebagainya.
3. Hash Function
   Fungsi Hash sering disebut fungsi hash satu arah (*one-way function*), *message digest, finger print,* fungsi kompresi, dan *authentication code* (MAC), merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap.

2.1.3 Kriptografi Klasik

Kriptografi klasik merupakan suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Kriptografi klasik memiliki beberapa ciri, yaitu :

1. Berbasis karakter
2. Menggunakan pena dan kertas saja, belum ada komputer
3. Termasuk ke dalam kriptografi kunci simetri

2.1.4 Kriptografi Modern

Kriptografi modern mempunyai kerumitan yang sangat kompleks karena dioperasikan menggunakan komputer. Algoritma kriptografi modern tidak lagi mengandalkan kemanannya pada kerahasiaan algoritma tetapi kerahasiaan kunci. *Plaintext* yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan *chipertext* yang berbeda pula. Algoritma kriptografi dapat bersifat umun dan boleh diketahui oleh siapa saja, akan tetapi tanpa pengetahuan tentang kunci, data tersandi tetap saja tidak dapat terpecahkan.

Berdasarkan besar data yang diolah dalam satu kali proses, maka algoritma kriptografi dapat dibedakan menjadi dua jenis, yaitu :

1. Algoritma block chiper
   Informasi yang hendak dikirim dalam bentuk blok-blok besar (misalnya 64 bit) dimana blok-blok ini dioperasikan dengan fungsi enkripsi yang sama dan akan menghasilkan informasi rahasia dalam blok-blok yang berukuran sama pula.
2. Algoritma stream chiper
   Informasi yang hendak dioperasikan dalam bentuk yang lebih kecil (byte atau bit), biasanya satu karakter persatuan waktu proses menggunakan transformasi enkripsi yang berubah setiap waktu.

2.2 Algoritma

Ditinjau dari asal-usulnya, kata algoritma mempunyai sejarah yang menarik.Kata ini muncul di dalam kamus *Webster* sampai akhir tahun 1957. Kata *algorism* mempunyai arti proses perhitungan dalam bahasa Arab. Algoritma berasal dari nama penulis buku Arab terkenal, yaitu Abu Ja'far Muhammad Ibnu Musa al-Khuwarizmi (al-Khuwarizmi dibaca oleh orang barat sebagai *algorism*). Kata algorism lambat laun berubah menjadi *algorithm*. Definisi terminologi algoritma adalah urutan langkah-langkah logis untuk menyelesaikan masalah yang disusun secara sistematis.

2.3 Algoritma ElGamal

Algoritma ElGamal merupakan algoritma yang termasuk dalam kategori algoritma asimetris. Keamanan algoritma ElGamal terletak pada kesulitan penghitungan logaritma diskrit pada bilangan modulo prima yang besar sehingga sukar diselesaikan [5]. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan dekripsi

2.3.1 Proses Pembentukan Kunci

Pembentukan kunci terdiri atas pembentukan kunci publik dan kunci rahasia. Proses ini dibutuhkan sebuah bilangan prima *p* yang digunakan untuk membentuk grup Zp*, elemen primitif α dan sembarang $a \in \{0,1,..., p-2\}$.Kunci publik algoritma ElGamal terdiri atas pasangan 3bilangan (*p*,α,β) di mana $\beta = \alpha^a \bmod p$ ….(1)

Sedangkan kunci rahasianya adalah bilangan *a* tersebut.Proses pembentukan kunci untuk algoritma ElGamal terdiri atas:

a. Penentuan bilangan prima aman yang bernilai besar
b. Penentuan elemen primitif
c. Pembentukan kunci berdasarkan bilangan prima aman dan elemen primitif

Penentuan bilangan prima aman besar

Tujuan penentuan bilangan prima aman ini adalah untuk mempermudah dalam penentuan elemen primitif. Digunakan bilangan prima *p* sehingga

$p = 2.q + 1$ .....(2)

dengan *q* adalah bilangan prima sehingga nilai minimal *p* adalah 5 dan *q* adalah 2. Bilangan prima *p* tersebut disebut sebagai bilangan prima aman. Langkah penentuan bilangan prima tersebut dinyatakan sebagai berikut:

a. Tentukan bilangan prima $p \geq 5$
b. Hitung *q* dengan "persamaan (2)"
c. Jika *q* merupakan bilangan prima, maka *p* merupakan bilangan prima aman.
d. Jika *q* bukan merupakan bilangan prima, maka *p* bukan merupakan bilangan prima aman. Untuk menguji keprimaan bilangan digunakan metode yang disebut Teorema Fermat.

Teorema Fermat

Jika *x* adalah bilangan prima dan *y* adalah bilangan bulat yang tidak habis dibagi dengan *x*, yaitu PBB (*y,x*) = 1, maka $y^{x-1} \equiv 1 \ (mod\ p)$.. (3)

Contoh pengujian keprimaan suatu bilangan.

Diuji apakah 17 dan 21 bilangan prima atau bukan. Kemudian diambil nilai *a* = 2 karena PBB(17,2) = 1 danPBB(21,2) = 1.

Untuk 17,

$2^{17-1} = 65536 = 1 \ (mod\ 17)$ Karena 17 habis membagi $65536 - 1 = 65535 (65535 \div 17 = 3855)$

Untuk 21,

$2^{21-1} = 1048576 \equiv \backslash 1 (mod\ 21)$ Karena 21 tidak habis membagi 1048576 – 1 = 1048576.

Akan tetapi, teorema ini memiliki kekurangan karena terdapat bilangan komposit *n* sedemikian sehingga $2^{n-1} \equiv 1 (mod\ n)$. Bilangan itu disebut bilangan prima semu (*pseudoprimes*). Misalnya komposit 341 (yaitu 341 = 11.31) adalah bilangan prima semu menurut teoreme Fermat,

$2^{340} \equiv 1 (mod\ 340)$Namun, bilangan prima semu ini relatif jarang terdapat.

Penentuan elemen primitif

Teorema:

"Suatu elemen yang membangun *Zp* * disebut *elemen primitif (primitive root) mod p*"."Bila $\alpha^2 \bmod p \neq 1$ dan $\alpha^q \bmod p \neq 1$.Jika keduanya dipenuhi, maka α adalah elemen primitif dari *Zp* *."

Langkah–langkah penentuan elemen primitif tersebut dapat dinyatakan sebagai berikut:

a. Tentukan bilangan prima $p \geq 5$ dan $\alpha \in Zp^*$
b. Hitung *q* dengan "persamaan (2)"
c. Hitung $\alpha^2 \bmod p$ dan $\alpha^q \bmod p$.
d. Jika $\alpha^2 \bmod p = 1$ atau $\alpha^q \bmod p = 1$, maka α bukan elemen primitif.
e. Jika $\alpha^2 \bmod p \neq 1$ dan $\alpha^q \bmod p \neq 1$, maka α merupakan elemen primitif.

2.3.2 Pembentukan Kunci Berdasarkan Bilangan Prima Aman Dan Elemen Primitif

Setelah bilangan prima aman dan elemen primitif diperoleh, kunci publik dan kunci rahasia untuk algoritma ElGamal dapat dibentuk. Algoritma ElGamal dalam prosesnya menggunakan bilangan bulat untuk perhitungan. Oleh karena itu, pesan yang terkandung dalam plainteks harus dalam bentuk bilangan bulat. Untuk memenuhi persyaratan tersebut, digunakan kode ASCII *(American Standard for Information Interchange)*yang merupakan representasi numeric dari karakter-karakter yang digunakan pada komputer, serta mempunyai nilai minimal 0 dan maksimal 255. Selanjutnya, dengan kondisi-kondisi tersebut, pembentukan kunci dapat dibentuk dengan mengacu pada langkah berikut:

a. Tentukan bilangan prima $p \geq 5$ dan $\alpha \in Zp^*$
b. Pilih *a* ∈{0,1,..., *p* − 2} sembarang.
c. Hitung nilai β dengan rumus $\beta = \alpha^a \bmod p$ (4)

Diperoleh kunci publik (*p*, α ,β) yang dapat dipublikasikan serta nilai kunci rahasia *a* yang dirahasiakan nilainya. Pihak yang membuat kunci publik dan kunci rahasia merupakan pihak penerima pesan. Sedangkan pihak pengirim hanya mengetahui kunci publik dari penerima untuk mengenkripsi pesan yang akan dikirim.

2.3.3 Proses Enkripsi

Proses enkripsi menggunakan kunci publik (*p*,α,β) dan sebuah bilangan integer acak *k* (*k* ∈{0,1,..., *p* − 1}) yang dijaga kerahasiaannya oleh penerima yang mengenkripsi pesan. Untuk setiap karakter dalam pesan dienkripsi dengan menggunakan bilangan k yang berbeda-beda. Satu karakter yang direpresentasikan dengan menggunakan bilangan bulat ASCII akan menghasilkan kode dalam bentuk blok yang terdiri atas dua nilai (*r*, *t*). Langkah proses enkripsi:

a. Ambil sebuah karakter dalam pesan yang akan dienkripsi dan transformasi karakter

tersebut kedalam kode ASCII sehingga diperoleh bilangan bulat *M*

b. Hitung nilai *r* dan *t* dengan persamaan berikut:
   $r = \alpha^{k} \pmod p$ ….(5)
   $t = \beta^{k} M \pmod p$ ….(6)
c. Diperoleh cipherteks untuk karakter *M* tersebut dalam blok (*r, t*)
d. Lakukan proses di atas untuk seluruh karakter termasuk karakter spasi.

2.3.4 Proses Dekripsi

Dekripsi dari cipherteks ke plainteks menggunakan kunci rahasia *a* yang disimpan kerahasiaanya oleh penerima pesan.

Teorema:

Diberikan (*p*, α, β) sebagai kunci public dan *a* sebagai kunci rahasia pada algoritma ElGamal. Jika diberikan cipherteks (*r, t*), maka $M = t\,(r^{a})^{-1} \bmod p$ …(7)
dengan *M* adalah plainteks.
Di mana nilai $(r^{a})^{-1} = r^{-a} = r^{p-1-a} \bmod p$… (8)
Langkah proses dekripsi:

a. Ambil sebuah blok cipherteks dari pesan yang telah dienkripsikan pengirim
b. Dengan menggunakan *a* yang dirahasiakan oleh penerima, hitung nilai plainteks dengan menggunakan "persamaan (7)" dan "persamaan (8)"

2.4 Algoritma Vigenere Chiper

Kode Vigenere termasuk kode abjad-majemuk (*polyalphabetic subsitution chiper*). Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenere pada abad 16 tahun 1586. Sebenarnya Giovan Batista Belaso telah menggambarkannya untuk pertama kali pada tahun 1553 seperti ditulis didalam buku *La Cifra del Sig*. Algoritma ini baru dikenal luas 200 tahun kemudian dan dinamakan kode Vigenere.

A	B	C	D	E	F	H	I	J	K	L	M	N
0	1	2	3	4	5	7	8	9	10	11	12	13
O	P	Q	R	S	T	U	V	W	X	Y	Z	T
14	15	16	17	18	19	20	21	22	23	24	25	19

Jika ditukar dengan angka, maka kunci huruf " HARI" menjadi K = (7, 0, 17, 8)

Plaintext	S	A	Y	A	H	A	R	I	Y	A	N	T	O
Plaintext	18	0	24	0	7	0	17	8	24	0	13	19	14
Kunci	7	0	17	8	7	0	17	8	7	0	17	8	7
Chipertext	25	0	15	8	14	0	8	16	5	0	4	1	22

Untuk melakukan deskripsi, bisa juga digunakan modulo 26

Tabel 1 Vigenere Cipher dengan huruf berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser ke kiri dari baris sebelumnya membentuk ke-26 kemungkinan sandi *Caesar* setiap huruf disediakan dengan menggunakan baris yang berbeda-beda sesuai kunci yang diulang.

Tabel 1 Vigenere Cipher dengan huruf

	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

Rumus enkripsi vigenere cipher :
Ci = (Pi + Ki) mod 26 (9)
Rumus dekripsi vigenere cipher :
untuk Ci > = Ki
Pi = (Ci – Ki) mod 26 (10)
untuk Ci < = Ki
Pi = (Ci+ 26 – Ki) mod 26 (11)
Keterangan:
C = Chiphertext ;P = Plaintext ; K = Kunci

PEMBAHASAN

3.1 Analisa Sistem

Salah satu cara untuk mengamankan pesan salah satunya dengan melakukan penyandian teks menggunakan algoritma kriptografi tertentu. Penyandian dilakukan dengan cara mengubah teks sebelum dikirim sehingga pesan awal berubah menjadi huruf atau angka acak yang tidak memiliki arti proses ini disebut enkripsi. Setelah pesan sampai kepada penerima maka penerima juga harus mengubah pesan acak tersebut menjadi pesan asli yang mengandung arti menggunakan algoritma yang sama seperti saat pengubahan pesan asli ke pesan acak yang disebut dengan deskripsi.

3.2 Analisa Penerapan Algoritma

1. Algoritma Vigenere Chiper
   a. Menggunakan Angka
      Penggunaan angka didasarkan pada jumlah huruf alfabet. Penomoran dimulai dari huruf A yang diberi angka 0 dan di akhiri dengan huruf Z dengan angka 25

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext= semangat skripsi ⟶ 18 4 12 0 13 6 0 19 18 10 17 8 15 18 8
Kunci= dan ⟶ 3 0 13
Maka

18	4	12	0	13	6	0	19	18	10	17	8	15	18	8	
3	0	13	3	0	13	3	0	13	3	0	13	3	0	13	+
21	4	25	3	13	19	3	19	5	13	17	21	18	18	21	

Chipertext = 21 4 25 3 13 19 3 19 5 13 17 21 18 18 21 ⟶ vezdntdtfnrvssv

b. Menggunakan Huruf

$C_1 = (P_1 + K_1) \bmod 26$
$= (S + D) \bmod 26$
$= (18 + 3) \bmod 26$
$= 21 \bmod 26 = 21 = V$
$C_2 = (P_2 + K_2) \bmod 26$
$= (E + A) \bmod 26$
$= (4 + 0) \bmod 26$
$= 4 \bmod 26 \quad = 4 = E$
$C_3 = (P_3 + K_3) \bmod 26$
$= (M + N) \bmod 26$
$= (12 + 13) \bmod 26$
$= 25 \bmod 26 = 25 = Z$
$C_4 = (P_4 + K_4) \bmod 26$
$= (A + D) \bmod 26$
$= (0 + 3) \bmod 26$
$= 3 \bmod 26 = 3 = D$
$C_5 = (P_5 + K_6) \bmod 26$
$= (N + A) \bmod 26$
$= (13 + 0) \bmod 26$
$= 13 \bmod 26 = 13 = N$
$C_6 = (P_6 + K_6) \bmod 26$
$= (G + N) \bmod 26$
$= (6 + 13) \bmod 26$
$= 19 \bmod 26 = 19 = T$
$C_7 = (P_7 + K_7) \bmod 26$
$= (A + D) \bmod 26$
$= (0 + 3) \bmod 26$
$= 3 \bmod 26 = 3 = D$
$C_8 = (P_8 + K_8) \bmod 26$
$= (T + A) \bmod 26$
$= (19 + 0) \bmod 26$
$= 19 \bmod 26 = 19 = T$
$C_9 = (P_9 + K_9) \bmod 26$
$= (S + N) \bmod 26$
$= (18 + 13) \bmod 26$
$= 31 \bmod 26 = 5 = F$
$C_{10} = (P_{10} + K_{10}) \bmod 26$
$= (K + D) \bmod 26$
$= (10 + 3) \bmod 26$
$= 13 \bmod 26 = 13 = N$
$C_{11} = (P_{11} + K_{11}) \bmod 26$
$= (R + A) \bmod 26$
$= (17 + 0) \bmod 26$
$= 17 \bmod 26 = 17 = R$
$C_{12} = (P_{12} + K_{12}) \bmod 26$
$= (I + N) \bmod 26$
$= (8 + 13) \bmod 26$
$= 21 \bmod 26 = 21 = V$
$C_{13} = (P_{13} + K_{13}) \bmod 26$

Berdasarkan tabel 2 Vigenere Cipher dengan huruf jika;
Plaintext = semangatskripsi
Kunci = dandandandandan
Maka *Chipertext* = vezdntdtfnrvssv

c. Menggunakan Rumus

Plaintext = semangatskripsi ; Kunci = dan

Enkripsi

$Ci = (Pi + Ki) \bmod 26$

$= (P + D) \bmod 26$
$= (15 + 3) \bmod 26$
$= 18 \bmod 26 = 18 = S$
$C_{14} = (P_{14} + K_{14}) \bmod 26$
$= (S + A) \bmod 26$
$= 18 \bmod 26 = 18 = S$
$C_{15} = (P_{15} + K_{15}) \bmod 26$
$= (I + N) \bmod 26$
$= (8 + 13) \bmod 26$
$= 21 \bmod 26 = 21 = V$
Chipertext =VEZDNTDTFNRVSSV

Deskripsi

untuk $Ci >= Ki \rightarrow Pi = (Ci - Ki) \bmod 26$
untuk $Ci < = Ki \rightarrow Pi = (Ci + 26 - Ki) \bmod 26$

$C_1 = 21 ; \ K_1 = 3$
$P_1 = (C_1 - K_1) \bmod 26$
$= (21-3) \bmod 26$
$= 18 \bmod 26 = 18 = S$
$C_2 = 4 ; \ K_2 = 0$
$P_2 = (C_2 - K_2) \bmod 26$
$= (4-0) \bmod 26$
$= 4 \bmod 26 = 4 = E$
$C_3 = 25 ; \ K_2 = 13$
$P_3 = (C_3 - K_3) \bmod 26$
$= (25-13) \bmod 26$
$= 12 \bmod 26 = 12 = M$
$C_4 = 3 ; \ K_4 = 3$
$P_4 = (C_4 - K_4) \bmod 26$
$= (3-3) \bmod 26$
$= 0 \bmod 26 = 0 = A$
$C_5 = 13 ; \ K_5 = 0$
$P_5 = (C_5 - K_5) \bmod 26$
$= (13-0) \bmod 26$
$= 13 \bmod 26 = 13 = N$
$C_6 = 19 ; \ K_3 = 13$
$P_6 = (C_6 - K_6) \bmod 26$
$= (19-13) \bmod 26$
$= 6 \bmod 26 = 6 = G$
$C_7 = 3 ; \ K_7 = 3$
$P_7 = (C_7 - K_7) \bmod 26$
$= (3-3) \bmod 26$
$= 0 \bmod 26 = 0 = A$
$C_8 = 19 ; \ K_8 = 0$
$P_8 = (C_8 - K_8) \bmod 26$
$= (19-0) \bmod 26$
$= 19 \bmod 26 = 19 = T$
$C_9 = 5 ; \ K_9 = 13$

$P_9 = (C_9 + 26 - K_9) \bmod 26$
$=(5+26-13) \bmod 26$
$=18 \bmod 26 = 8 = S$
$C_{10} = 13 ; \ K_2 = 3$
$P_{10} = (C_{10} - K_{10}) \bmod 26$
$=(13-3) \bmod 26$
$=10 \bmod 26 = 10 = K$
$C_{11} = 17 ; \ K_{11} = 0$
$P_{11} = (C_{11} - K_{11}) \bmod 26$
$=(17-0) \bmod 26$
$=17 \bmod 26 = 17 = R$
$C_{12} = 21 ; \ K_{12} = 13$
$P_{12} = (C_{12} + 26 - K_{12}) \bmod 26$
$=(21+26-13) \bmod 26$
$=34 \bmod 26 = 8 = I$

2. Algoritma ElGamal

I. Pembentukan Kunci

a. Penentuan bilangan prima

$p \geq 5 \rightarrow p = 167$
$p = 2q + 1$
$167 = 2q + 1$
$q = -166/2 = 83$

Karena $q=83$ merupakan bilangan prima maka $p=167$ merupakan bilangan prima aman.

b. Penentuan elemen primitif

$p=167 \ ; \ q=83$
$a \in (0,1,2,.....p-2)$
$a \in (0,1,2,.....165)$ } $\alpha = 73$

Sehingga di dapat kunci publik $(p,\alpha,\beta) = (167,5,113)$ dan kunci pribadi $a = 73$

II. Enkripsi

a. Ubah dalam bentuk ASCII

Plaintext = SEMANGAT SKRIPSI

b. Menentukan bilangan acak $k \in (0,1,2,3,4,...p-1)$ maka k adalah $\{0,1,2,3,.....166\}$

c. Menghitung nilai r dan t

Tabel 3 Konversi karakter ke kode ASCII

I	Karakter	Plainteks M_i	ASCII
1	S	M_1	83
2	E	M_2	69
3	M	M_3	77
4	A	M_4	65
5	N	M_5	78
6	G	M_6	71
7	A	M_7	65
8	T	M_8	84
9	(spasi)	M_9	32
10	S	M_{10}	83
11	K	M_{11}	75
12	R	M_{12}	82
13	I	M_{13}	73
14	P	M_{14}	80
15	S	M_{15}	83
16	I	M_{16}	73

$r = \alpha^k \pmod p$
$= 5^k \pmod{167}$
$t = \beta^k M \pmod p$
$= 113^k M \pmod{167}$

Tabel 4 Enkripsi Plainteks ke Cipherteks

$C_{13} = 18 ; \ K_2 = 3$
$P_{13} = (C_{13} - K_{13}) \bmod 26$
$=(18-3) \bmod 26$
$=15 \bmod 26 = 15 = P$

$C_{14} = 18 ; \ K_{14} = 0$
$P_{14} = (C_{14} - K_{14}) \bmod 26$
$=(18-0) \bmod 26$
$=18 \bmod 26 = 18 = S$
$C_{15} = 21; \ K_{15} = 13$
$P_{15} = (C_{15} - K_{15}) \bmod 26$
$=(21-13) \bmod 26$
$=8 \bmod 26 = 8 = I$
Plaintext = SEMANGAT SKRIPSI

Tabel 2 Penghitungan $\alpha^2 \bmod p$ dan $\alpha^q \bmod p$

A	2	3	4	5	6
$\alpha^2 \bmod p$	4	9	16	25	36
$\alpha^q \bmod p$	1	1	1	166	1

Elemen primitif yaitu $\alpha=5$ karena pada 2,3,4,6 terdapat $\alpha^2 \bmod p = 1$ atau $\alpha^q \bmod p = 1$

c. Penentuan kunci berdasarkan bilangan prima dan elemen primitif

$p=167; \ q=83 \ ; \ \alpha=5$

$\beta = \alpha^a \bmod p$
$= 5^{73} \bmod 167 = 113$

I	M_i	k_i	$r = 5^k \pmod{167}$	$t = 113^k M \pmod{167}$
1	83	63	90	16
2	69	70	49	103
3	77	50	99	130
4	65	43	83	73
5	78	76	97	148
6	71	81	20	88
7	65	52	137	100
8	84	35	160	123
9	32	80	4	116
10	83	65	79	63
11	75	87	43	46
12	82	57	104	88
13	73	88	48	134
14	80	34	32	118
15	83	69	110	115
16	73	87	43	47

Berdasarkan tabel 4 diperoleh cipherteks (r_i, t_i), i = 1, 2, 3,4,5,…, 14, 15, 16 adalah (90, 16), (49, 103), (99, 130), (83, 73), (97, 148), (20, 88), (137, 100), (160, 123), (4, 116), (79, 63), (43, 46), (104, 88), (48, 134), (32, 118), (110, 115) dan (43, 47)

III. Deskripsi

a. Menghitung M sebagai plaintext dengan kunci rahasia $(a)= 73$

$M = t (r^a)^{-1} \bmod p$ dimana
$(r^a)^{-1} = r^{-a} = r^{p-1-a} \bmod p$
$= r^{167-1-73} \bmod 167$
$= r^{93} \bmod 167$

Tabel 5 Dekripsi Cipherteks ke Plainteks

i	r	T	I^{83} (mod 167)	M_i= t $(r^a)^{-1}$(mod 167)	Karakter Mi
1	90	16	120	83	S
2	49	103	132	69	E
3	99	130	25	77	M
4	83	73	129	65	A
5	97	148	75	78	N
6	20	88	90	71	G
7	137	100	9	65	A
8	160	123	74	84	T
9	4	116	150	32	(spasi)
10	79	63	110	83	S
11	43	46	165	75	K
12	104	88	111	82	R
13	48	134	99	73	I
14	32	118	12	80	P
15	110	115	53	83	S
16	43	47	165	73	I

Plainteks *Mi* = 1, 2, , 16 adalah 83, 69, 77, 65, 78, 71, 65, 84, 32, 83, 75, 82, 73, 80, 83, 73 jika di ubah dalam ASCII menjadi SEMANGAT SKRIPSI

KESIMPULAN

Berdasarkan pembahasan penelitian ini dapat ditarik kesimpulan sebagai berikut :

1. Penyandian dilakukan dengan cara mengubah teks sebelum dikirim sehingga pesan awal berubah menjadi huruf atau angka acak yang tidak memiliki arti proses ini disebut enkripsi. Setelah pesan sampai kepada penerima maka penerima juga harus mengubah pesan acak tersebut menjadi pesan asli yang mengandung arti menggunakan algoritma yang sama seperti saat pengubahan pesan asli ke pesan acak yang disebut dengan deskripsi
2. Proses enkripsi dengan algoritma Elgamal menggunakan kunci publik dan proses deskripsinya menggunakan kunci rahasia. Sedangkan Vigenere Chiper hanya menggunakan satu kunci yang sama untuk proses enkripsi dan deskripsinya.
3. Perancangan aplikasi penyandian pesan teks menggunakan android *Ice Cream Sandwich* (4.0.3), emulator *platform* Android SDK sebagai *virtual device* dan ADT Eclipse

DAFTAR PUSTAKA

1. Ariyus, Dony. (2008). Pengantar Ilmu KRIFTOGRAFI Teori, Analisis, dan Implementasi. Yogyakarta:ANDI
2. Arjana, Putu H., Tri Puji Rahayu., Yakub., Hariyanto. 2012. “Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper”.Seminar Nasional Teknologi Informasi dan Komunikasi 2012 (SENTIKA 2012). 2089-9815,165-166.
3. Dengen, Nataniel., Heliza Rahmania Hatta. 2009. “Perancangan Sistem Informasi Terpadu Pemerintah Daerah Kabupaten Paser”.Jurnal Informatika Mulawarman.. 2089-9815,48.
4. Dilihatya.com, Informasi Online, Retrieved May 02 , 2015, from http://dilihatya.com/1178/pengertian-aplikasi-menurut-para-ahli
5. Ifanto, Mukhammad, 2009. “Metode Enkripsi Dan Dekripsi Dengan Menggunakan Algoritma Elgamal”. Makalah If2091 Struktur Diskrit.2-4.
6. Kromodimoeljo, Sentot. (2009). Teori dan Aplikasi Kriptografi. Yogyakarta:SPK IT Consulting
7. Komputer_Wahana. (2013). Step by Step Menjadi Pemrograman Android, Yogyakarta:ANDI
8. Metode dan Algoritma, Retrieved May 02 , 2015, from http://www.metode-algoritma.com/2013/06/algoritma-kriptografi.html
9. Nugroho, Adi. (2010). Rekayasa Perangkat Lunak Berorientasi Objek dengan Metode USDP, Yogyakarta:ANDI
10. panduaji, Retrieved May 03 , 2015, fromhttp://www.panduaji.net/2011/11/tutorial-dasar-eclipse.html
11. Rachmat, Antonius C. (2010). Algoritma dan Pemrograman dengan Bahasa C-Konsep, Teori, & Implementasi. Yogyakarta:ANDI
12. Rahman’s personal Blog, Blog Tutorial Coding Indonesia, Retrieved May 18, 2015, fromhttp://rahmansurya.net/teknik-dasar-kriptografi/
13. Sahidin, Rifky. (2012). Kriptografi untuk keamanan jaringan, Yogyakarta:ANDI
14. Saputra, Agus, (2011). Step By Step Membangun Aplikasi SMS dengan PHP dan Mysql. Jakarta:PT. Alex Media Komputindo
15. Sugiarti,Yuni. (2013). ANALISIS DAN PERANCANGAN UML (Unified Modeling Languange) Generated VB. 6, Yogtakarta:Graha Ilmu
16. Satyaputra, Alfa. M.Sc. dan Eva.Maulina.Aritonang. S.Kom. (2012). JAVA for Beginners with Eclipse 4.2 Juno, Jakarta: PT. Alex Media Komputindo