Analisa Pengamanan Kata Dengan Algoritma Elgamal

Aida Indriani
Program Studi Teknik Informatika
STMIK PPKIA Tarakanita Rahmawati
Tarakan
aida@ppkia.ac.id

Muhammad
Program Studi Sistem Informasi
STMIK PPKIA Tarakanita Rahmawati
Tarakan
muhammad@ppkia.ac.id

Abstrak*— Pada dewasa ini, keamanan merupakan hal yang sangat penting dalam kehidupan sehari-hari. Pengamanan dilakukan untuk menjaga data/informasi yang bersifat rahasia agar tidak jatuh kepada pihak yang tidak berkepentingan. Data/informasi dapat berupa teks, audio, video maupun gambar. Dalam melakukan pengamanan data dapat menggunakan beberapa teknik yang dirancang untuk melindungi data yang ada. Ada 2 (dua) teknik yang sering digunakan dalam hal pengamanan data yaitu teknik kriptografi dan steganoraphy. Kriptografi yaitu teknik pengacakan data menjadi data yang tidak mempunyai makna, sedangkan steganography yaitu teknik penyembunyian data kedalam media lain. Dari teknik kunci, kriptografi terbagi atas 2 (dua) jenis yaitu kriptografi kunci simetri dan asimetri. Kunci simetri yaitu kunci yang digunakan pada proses enkripsi dan dekripsi adalah sama, sedangkan kunci asimetri menggunakan 2 (dua) kunci yang berbeda yaitu kunci publik dan privat. Pada penelitian ini, penulis melakukan analisa pengamanan kata (teks) dengan menggunakan algoritma ElGamal yang termasuk dalam kriptografi kunci asimetri dan blok cipher. Pada penelitian ini, analisa yang dilakukan dari plainteks yang ada menjadi blok cipherteks melalui proses enkripsi dengan menggunakan kunci publik (y, g, p) dan kembali menjadi plainteks melalui proses dekripsi dengan menggunakan kunci privat (x, p). untuk membantu proses perhitungan perpangkatan dengan nilai besar, penulis menggunakan perhitungan perpangkatan biner.

Kata kunci—kriptografi; algoritma elgamal; pangkat biner; kunci asimetri

I. PENDAHULUAN

Informasi adalah data mentah yang diolah menjadi sebuah bentuk yang mempunyai makna. Informasi dapat bersifat biasa/umum atau rahasia. Informasi rahasia tidak akan menjadi rahasia lagi apabila telah diambil oleh pihak yang tidak berkepentingan. Pada zaman sekarang, keamanan pada jaringan internet sudah tidak begitu aman. Telah banyak pihak-pihak yang tidak berkepentingan mengambil informasi melalui jalur internet, dan dampaknya sangat merugikan banyak pihak. Yang bisa dilakukan untuk mengatasi pencurian informasi melalui jalur internet adalah bagaiman melakukan pengamanan terhadap informasi yang akan dikirim oleh pihak pengirim kepada pihak penerima. Dengan harapan, walaupun informasi tersebut diambil oleh pihak yang tidak berkepentingan tetapi tetap tidak dapat digunakan karena informasi yang dikirim juga telah diamankan. Dan akhirnya akan meminimalkan penyebaran informasi rahasia ke masyarakat umum.

Pengamanan informasi dapat menggunakan 2 (dua) teknik yaitu kriptografi dan steganografi. Kriptografi adalah teknik pengamanan dengan mengubah informasi yang awalnya mempunyai arti menjadi tidak berarti. Sedangkan steganography adalah teknik pengamanan informasi dengan menyembunyikan ke dalam sebuah media penampung. Yang dimaksud dengan media penampung dalam teknik steganography dapat berupa teks, gambar, audio, dan video. Pengamanan dapat juga menggunakan gabungan dari 2 (dua) teknik yaitu dengan cara melakukan kriptografi kemudian hasil dari kriptorafi dilakukan teknik steganography dengan media penampung.

Teknik pengamanan informasi dengan menggunakan kriptografi lebih banyak dilakukan karena hanya mengolah informasi itu sendiri tidak perlu menggunakan media penampung. Pengamanan informasi dilakukan dengan menggunakan kriptografi dan penggunaan kunci asimetri. Tujuannya yaitu bagaimana melakukan perubahan kata yang terdapat pada informasi menjadi informasi yang tidak mempunyai makna sehingga kerahasiaan informasi dapat terhindar dari pihak yang tidak berkepentingan. Algoritma kriptografi yang digunakan yaitu algoritma ElGamal.

Dengan menggunakan algoritma ElGamal, pada penelitian ini penulis menjelaskan analisa pengamanan kata yang dimulai dari tahapan proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ElGamal merupakan algoritma kriptografi kunci asimetri yaitu dalam proses enkripsi dan dekripsi menggunakan kunci yang berbeda. Hal ini membuat algoritma ElGamal memiliki tingkat keamanan yang lebih dibanding dengan algoritma kriptografi kunci simetri. Dengan bantuan perhitungan perpangkatan biner, dapat mempermudah dalam proses enkripsi dan dekripsi. Uji coba yang dilakukan adalah mengamankan kata yang terdiri dari karakter/huruf yang yang disesuaikan dengan kebutuhan pengguna (tidak berdasarkan tabel ASCII).

II. KAJIAN PUSTAKA

Pada penelitian ini, penulis melakukan kajian pustaka terkait dengan beberapa teori yang digunakan untuk melakukan analisa pengamanan kata dengan teknik kunci asimetri.

A. Kriptografi

Kriptografi merupakan ilmu dan seni yang digunakan untuk menjaga pesan yang bersifat rahasia dengan teknik

menyandikannya menjadi bentuk yang tidak mempunyai makna. Kriptografi juga mempunyai banyak macam jenis. Kriptografi dapat dibedakan menurut sejarah menjadi kriptografi klasik dan modern. Kriptografi juga dapat dibedakan menurut cara pengerjaannya berdasarkan karakter atau blok. Selain itu juga kriptografi dapat dibedakan dari kunci (key) yang digunakan yaitu simetri atau asimetri. Pada kunci simetri hanya mengenal 1 (satu) kunci yang digunakan untuk kedua proses yaitu enkripsi dan dekripsi. Sedangkan pada kunci asimetri mengenal 2 (dua) kunci yaitu kunci publik yang digunakan untuk proses enkripsi dan kunci privat yang digunakan untuk proses dekripsi.

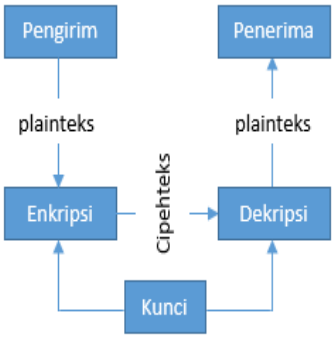
Dalam kriptografi, ada 2 (dua) proses yang biasa dilakukan yaitu proses enkripsi dan proses dekripsi. Plaintext (teks biasa) merupakan istilah yang digunakan untuk mewakili pesan yang akan dienkripsi. Plaintext merupakan informasi yang dapat dengan mudah dibaca dan dipahami oleh siapapun. Istilah yang digunakan untuk pesan plaintext yang telah dienkripsi yaitu ciphertext (teks sandi) [1].

Pada kriptografi, terdapat beberapa komponen yang biasa digunakan, antra lain:

1) Enkripsi merupakan proses pengamanan data yang terjaga kerahasiannya pada saat data dikirim.
2) Dekripsi merupakan proses pengembalian data yang telah dienkripsi menjadi bentuk aslinya.
3) Kunci adalah kunci yang digunakan dalam proses enkripsi dan dekripsi. Kunci dibedakan menjadi 2 (dua) yaitu kunci publik dan kunci privat.
4) Ciphertext (cipherteks) adalah pesan yang telah disandikan pada proses enkripsi. Pesan yang dihasilkan merupakan pesan yang tidak mempunyai makna.
5) Plaintext (plainteks) adalah pesan asli yang akan disandikan yang masih memiliki makna dan akan diubah menjadi cipherteks melalui proses enkripsi [2].

B. Kunci Simetri dan Asimetri

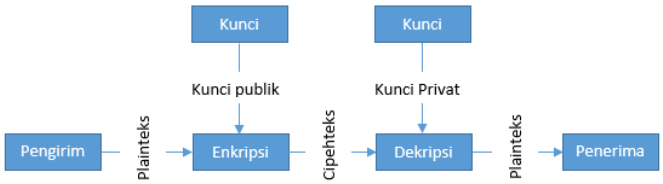
Kunci simetri dalam kriptografi adalah kunci yang digunakan untuk melakukan enkripsi dan dekripsi sama. Proses dari penggunaan kunci simetri yaitu pengirim dan penerima pesan saling mengetahui kunci yang digunakan. Skema kriptografi kunci simetri ditunjukkan pada gambar 1.



Gambar 1. Skema kriptografi kunci simetri

Kunci asimetri dalam kriptografi digunakan untuk menyelesaikan masalah distribusi kunci pada kunci simetri. Kunci asimetri diusulkan oleh Diffie dan Helman. Pada dasarnya, kunci asimetri menggunakan kunci yang berbeda pada proses enkripsi dan dekripsi. Kunci asimetri terdapat isitilah untuk kunci yang digunakan, antara lain:

1) Kunci publik, yaitu kunci yang memang sengaja diumumkan kepada publik dan disebarkan dengan bebas kepada semua orang.
2) Kunci privat, yaitu kunci yang hanya diketahui oleh pemilik kunci dan tidak untuk disebarkan kepada semua orang. Hanya orang-orang yang memiliki akses yang dapat memiliki kunci privat [3]. Skema kriptografi kunci asimetri ditunjukkan pada gambar 2.



Gambar 2. Skema kriptografi kunci asimetri

C. Algoritma ElGamal

Algoritma ElGamal pertama kali dipublikasikan oleh Taher ElGamal pada tahun 1985 [4]. Algoritma ElGamal merupakan algoritma kriptografi asimetri dengan mempunyai 2 (dua) kunci yaitu kunci publik dan kunci privat [5]. Algoritma ElGamal mempunyai 3 tahapan, yaitu pembentukan kunci, proses enkripsi, dan proses dekripsi [6].

Kunci yang digunakan pada algoritma ElGamal diperoleh dengan membangkitkan dua bilangan acak (random) g, x dan bilangan prima p, dimana bilangan g dan x lebih kecil dari nilai p dengan memenuhi persamaan seperti pada (1).

$$y = g^x \bmod p \qquad (1)$$

Dari persamaan (1), yang termasuk dalam pasangan kunci publik yaitu nilai y, g dan p, sedangkan yang termasuk dalam pasangan kunci privat yaitu nilai x dan p [7]. Variabel yang digunakan pada algoritma ElGamal antara lain:

1) p merupakan bilangan prima yang sifatnya tidak rahasia.
2) g merupakan bilangan acak pertama yang memenuhi syarat nilai g < p dan sifatnya tidak rahasia.
3) x merupakan bilangan acak kedua yang memenuhi syarat nilai x < p dan sifatnya rahasia (kunci privat).
4) $y = g^x \bmod p$ merupakan kunci publik yang sifatnya tidak rahasia.
5) m merupakan plainteks yang sifatnya rahasia.
6) a dan b merupakan cipherteks yang sifatnya tidak rahasia [5].

Proses enkripsi pada algoritma ElGamal dilakukan dengan cara memilih bilangan acak k dengan nilai yang berada dalam himpunan $1 \leq k \leq p-2$. Pada persamaan (2) dan (3) menunjukkan proses enkripsi plainteks m.

$$a = g^k \bmod p \quad (2)$$

$$b = y^k \, m \bmod p \quad (3)$$

Proses dekripsi pada algoritma ElGamal menggunakan kunci pribadi x dan p terhadap nilai a dan b menjadi plainteks m. Pada persamaan (4) dan (5) menunjukkan proses dekripsi cipherteks a dan b [7].

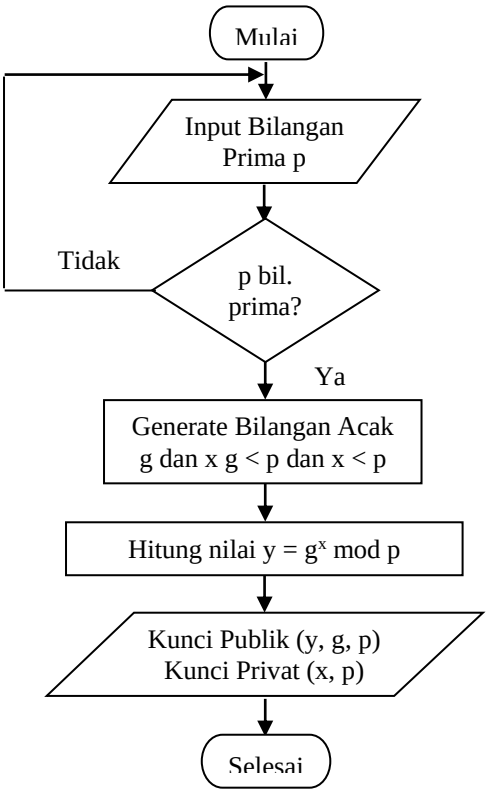
$$(ax)^{-1} = a^{p-1-x} \bmod p \quad (4)$$

$$m = b * (ax)^{-1} \bmod p \quad (5)$$

Dari penjelasan di atas, pengamanan data dengan algoritma ElGamal, menggunakan kunci yang berbeda untuk proses enkrpsi dan dekripsi. Hal ini membuat algoritma ElGamal memiliki tingkat keamanan yang lebih aman dibanding dengan menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Kelemahan dengan menggunakan kunci yang sama yaitu, pada saat kunci jatuh ditangan pihak lain, maka kerasahasiaan informasi dapat terbaca.

III. TAHAPAN ANALISA

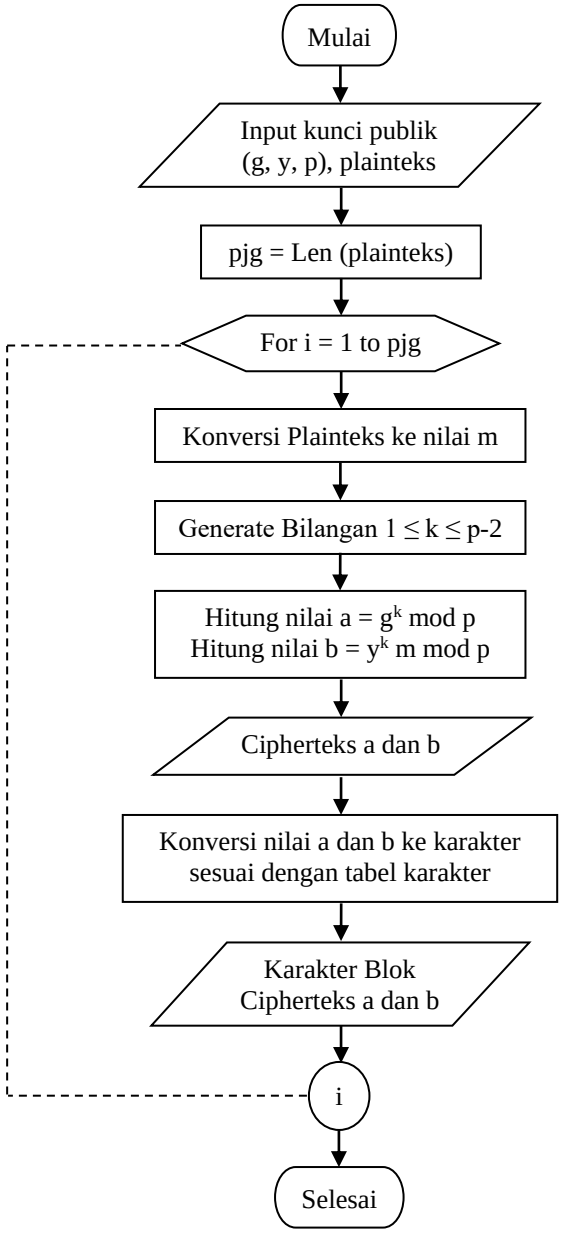
Tahapan analisa digunakan untuk menjelaskan langlah-langkah yang dikerjakan pada proses analisa pengaman kata dengan algoritma ElGamal. Adapun tahapan analisa dibagi menjadi 3 (tiga) proses yaitu proses pembentukan kunci publik dan privat, proses enkripsi dan proses dekripsi. Proses pembentukan kunci publik dan privat ditunjukkan pada gambar 3.



Gambar 3. Proses pembentukan kunci publik dan privat

Proses pembentukan kunci publik dan privat yang ditunjukkan pada gambar 3 yaitu dimulai dari penentuan bilangan prima yang disimbolkan dengan p, kemudian melakukan pengacakan bilangan untuk nilai g dan x dimana nilai g < p dan nilai x < p. Setelah mendapatkan nilai p, g dan x, langkah selanjutnya adalah menghitung nilai y yang diperoleh dari g^x mod p. Dari hasil perhitungan diperoleh 2 (dua) kunci yaitu kunci publik dengan nilai y, g dan p yang digunakan untuk proses enkripsi dan kunci privat dengan nilai x dan p yang digunakan untuk proses dekripsi.

Untuk proses enkripsi pada algoritma ElGamal ditunjukkan pada gambar 4.

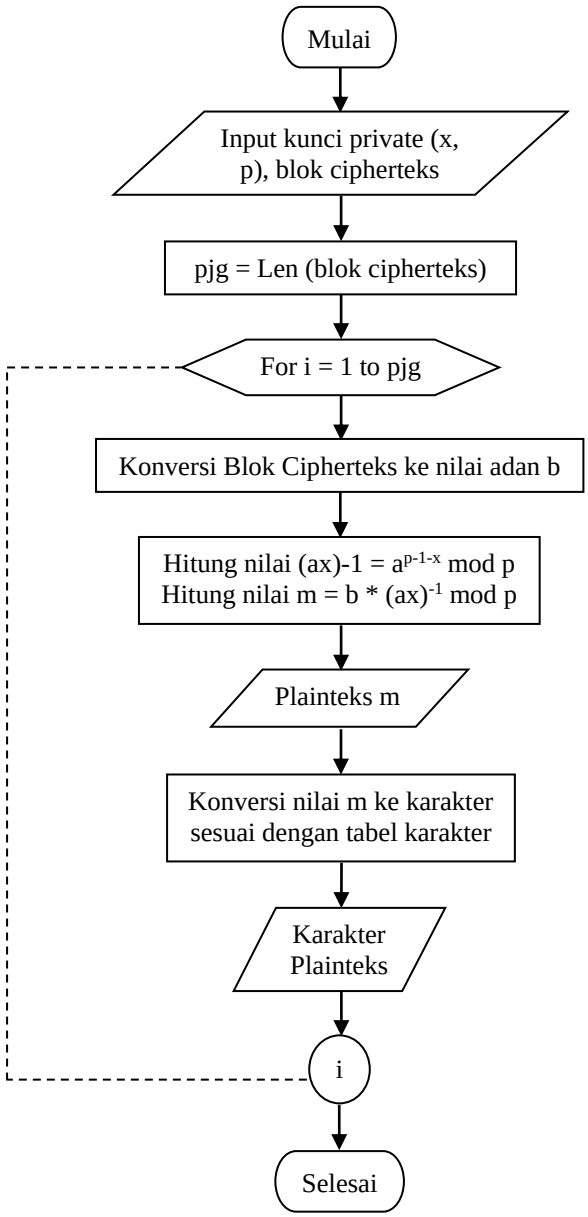


Gambar 4. Proses enkripsi algoritma ElGamal

Proses enkripsi algoritma ElGamal yang ditunjukkan pada gambar 4 yaitu dimulai dari penentuan nilai y, g dan p sebagai kunci publik dan karakter palinteks yang akan disandikan. Selanjutnya yaitu hitung panjang karakter yang akan disandikan dengan perintah len(plainteks) dengan variabel pjg.

Lakukan proses perhitungan enkripsi sepanjang karakter yaitu dimulai dari karakter pertama sampai dengan akhir karakter. Proses perhitungan enkripsi untuk setiap karakter dimulai dari mencari nilai konversi plainteks (m), dilanjutkan dengan membangkitkan bilangan k dengan kondisi $1 \leq k \leq p-2$ dan dilanjutkan dengan menghitung nilai a dan b yang merupakan nilai cipherteks. Nilai a diperoleh dari g^k mod p dan nilai b diperoleh dari y^k m mod p. Langkah terakhir konversi kembali nilai a dan b menjadi karakter.

Untuk proses dekripsi pada algoritma ElGamal ditunjukkan pada gambar 5.



Gambar 5. Proses dekripsi algoritma ElGamal

Proses dekripsi algoritma ElGamal yang ditunjukkan pada gambar 5 yaitu dimulai dari penentuan nilai x dan p sebagai kunci privat dan karakter blok cipherteks yang akan didekripsi. Selanjutnya yaitu hitung panjang karakter yang akan didekripsi dengan perintah len (blok cipherteks) dengan variabel pjg.

Lakukan proses perhitungan enkripsi sepanjang karakter yaitu dimulai dari karakter pertama sampai dengan akhir karakter. Proses perhitungan enkripsi untuk setiap karakter dimulai dari mencari nilai konversi plainteks (m), dilanjutkan dengan membangkitkan bilangan k dengan kondisi $1 \leq k \leq p-2$ dan dilanjutkan dengan menghitung nilai a dan b yang merupakan nilai cipherteks. Nilai a diperoleh dari g^k mod p dan nilai b diperoleh dari y^k m mod p. Langkah terakhir konversi kembali nilai a dan b menjadi karakter.

IV. HASIL DAN PEMBAHASAN

A. *Kunci Publik dan Private*

Diberikan sebuah bilangan prima (p) adalah 97. Nilai bilangan acak yang digenerate dari angka 1 s.d < p. Setelah melakukan proses generate bilangan diperoleh bilangan 5 untuk g dan 75 untuk x. Dari bilangan yang telah diperoleh, dilakukan perhitungan untuk mendapatkan nilai y dengan menggunakan persamaan (1).

$y = g^x \bmod p$
$y = 5^{75} \bmod 97$
$y = 63$

Dari perhitungan, diperoleh nilai y adalah 63. Dari nilai-nilai p, g, x dan y dibentuk pasangan kunci publik dan kunci privat. Kunci publik dengan menggunakan nilai-nilai y, g dan p (63, 5, 97) dan kemudian digunakan untuk proses enkripsi. Untuk kunci privat dengan menggunakan nilai-nilai x dan p (75, 97) dan kemudian digunakan untuk proses dekripsi.

B. *Enkripsi*

Untuk melakukan proses enkripsi, terlebih dahulu membuat sebuah nilai plainteks (m) dari karakter-karakter yang digunakan. Dalam penelitian ini, penulis tidak menggunakan nilai kode ASCII. Nilai plainteks (m) dari karakter yang digunakan ditunjukkan pada tabel I.

TABEL I. NILAI PLAINTEKS (M) DARI BEBERAPA KARAKTER

Karakter	**Nilai (m)**	**Karakter**	**Nilai (m)**
A	1	Blank(spasi)	53
B	2	!	54
C	3	…	…
…	…	0	69
Z	26	1	70
a	27	2	71
b	28	…	…
C	29	=	82
…	…	…	…
z	52	~	95

Diberikan sebuah plainteks “PPKIA”, proses enkripsi yang dilakukan dengan algoritma ElGamal adalah sebagai berikut:

Kunci publik (y, g, p) = 63, 5, 97. Hasil konversi dari setiap karakter dari plainteks yang diberikan adalah "P" = 16, "K" = 11, "I" = 9 dan "A" = 1 nilai-nilai tersebut diperoleh dari tabel I. Hasil perhitungan proses enkripsi ditunjukkan pada tabel II.

TABEL II. PERHITUNGAN PROSES ENKRIPSI ALGORITMA ELGAMAL

Plainteks	m	k	a	b	Cipherteks a	Cipherteks b
P	16	1	5	38	E	l
P	16	4	43	54	q	!
K	11	3	28	82	b	=
I	9	8	6	4	F	D
A	1	6	8	70	H	1

Nilai k pada tabel II diperoleh dari melakukan generate bilangan $1 \leq k \leq p-2$ untuk setiap karakter yang ada. Nilai a diperoleh dari persamaan (2) yaitu $a = g^k \bmod p$, proses perhitungan dijelaskan sebagai berikut:

untuk k = 1
$a = 5^1 \bmod 97 = 5$
untuk k = 4
$a = 5^4 \bmod 97 = 43$
untuk k = 3
$a = 5^3 \bmod 97 = 28$
untuk k = 8
$a = 5^8 \bmod 97 = 6$
untuk k = 6
$a = 5^6 \bmod 97 = 8$

Nilai b diperoleh dari persamaan (3) yaitu $b = y^k\ m \bmod p$, proses perhitungan dijelaskan sebagai berikut:

Untuk k = 1 dan m = 16
$b = (63^1 * 16) \bmod 97 = 38$
untuk k = 4 dan m = 16
$b = (63^4 * 16) \bmod 97 = 54$
untuk k = 3 dan m = 11
$b = (63^3 * 11) \bmod 97 = 82$
untuk k = 8 dan m = 9
$b = (63^8 * 9) \bmod 97 = 4$
untuk k = 6 dan m =1
$b = (63^6 * 1) \bmod 97 = 70$

Setelah mendapatkan nilai a dan b, selanjutnya yaitu mengkonversi nilai a dan b kekarakter yang tersedia pada tabel I. Sehingga memperoleh pasangan blok cipherteks yaitu El q! b= FD H1. Dengan algoritma ElGamal, proses enkripsi menghasilkan blok cipherteks yaitu plainteks yang terdiri dari 1 karakter menjadi 2 karakter dalam 1 blok. Hal ini membuat algoritma ElGamal berbeda dengan algorima pengamanan data lainnya yaitu 1 krakter plainteks tetap menghasilkan 1 karakter cipherteks.

C. Dekripsi

Proses dekripsi pada algoritma ElGamal dilakukan dengan menggunakan kunci privat yang diperoleh dari proses pembentukan kunci. Kunci privat yang terbentuk yaitu dari nilai x dan p (75, 97). Blok cipherteks yang terbentuk pada proses enkripsi yaitu El q! b= FD H1 dilakukan konversi untuk mendapatkan nilai cipherteks yang diperoleh dari tabel I. Blok karakter "El" = 5 38, "q!" = 43 54, "b=" = 28 82, "FD" = 6 4, "H1" = 8 70. Hasil perhitungan proses dekripsi ditunjukkan pada tabel III.

TABEL III. PERHITUNGAN PROSES DEKRIPSI ALGORITMA ELGAMAL

blok cipherteks	a	b	$(ax)^{-1}$	m	plainteks
El	5	38	77	16	P
q!	43	54	47	16	P
b=	28	82	51	11	K
FD	6	4	75	9	I
H1	8	70	79	1	A

Nilai (ax)-1 diperoleh dengan menggunakan persamaan (4) yaitu $(ax)^{-1} = a^{p-1-x} \bmod p$, proses perhitungan dijelaskan sebagai berikut:

untuk a = 5
$(ax)^{-1} = 5^{(97-1-75)} \bmod 97 = 77$
untuk a = 43
$(ax)^{-1} = 43^{(97-1-75)} \bmod 97 = 47$
untuk a = 28
$(ax)^{-1} = 28^{(97-1-75)} \bmod 97 = 51$
untuk a = 6
$(ax)^{-1} = 6^{(97-1-75)} \bmod 97 = 75$
untuk a = 8
$(ax)^{-1} = 8^{(97-1-75)} \bmod 97 = 79$

Nilai m diperoleh dengan menggunakan persamaan (5) yaitu $m = b * (ax)^{-1} \bmod p$, proes perhitungan dijelaskan sebagai berikut:

untuk b = 38
$m = (38 * 77) \bmod 97 = 2.926 \bmod 97 = 16$
untuk b = 54
$m = (54 * 47) \bmod 97 = 2.538 \bmod 97 = 16$
untuk b = 82
$m = (82 * 51) \bmod 97 = 4.182 \bmod 97 = 11$
untuk b = 4
$m = (4 * 75) \bmod 97 = 300 \bmod 97 = 9$
untuk b = 70
$m = (70 * 79) \bmod 97 = 5.530 \bmod 97 = 1$

Setelah mendapatkan nilai m, selanjutnya yaitu mengkonversi nilai m kekarakter yang tersedia pada tabel I. Sehingga memperoleh plainteks yaitu P P K I A. Dengan menggunakan algoritma ElGamal yang memiliki 2 (dua) kunci yang berbeda pada proses enkripsi dan dekripsi dapat menghasilkan plainteks yang sama dan membuat tingkat keamanan data lebih dibanding hanya dengan menggunakan algoritma kriptografi dengan 1 (satu) kunci yang sama.

D. Perpangkatan Biner

Perpangkatan dengan nilai besar terkadang menghasilkan pesan #NUM!. Untuk mengatasi perhitungan dengan pangkat yang terlalu besar dapat menggunakan bantuan perpangkatan biner. Sebagai contoh: $8^{(97-1-75)} \bmod 97$ = #NUM! jika menggunakan perhitungan biasa. Jika dihitung dengan

menggunakan perpangkatan biner, $8^{(97-1-75)} \bmod 97 = 79$. Adapun proses perhitungan perpangkatan biner dijabarkan sebagai berikut:

$8^{(97-1-75)} \bmod 97 = 8^{21} \bmod 97$

pangkat 21 dijabarkan dalam bentuk biner menjadi

128	64	32	16	8	4	2	1
0	0	0	1	0	1	0	1

pangkat tertinggi yang bernilai 1 adalah 16, jadi perhitungan dilakukan hanya sampai pangkat 16.

$1 = 8^1 \bmod 97 = 8$
$2 = 8^2 \bmod 97 = 64$
$4 = 64^2 \bmod 97 = 4.096 \bmod 97 = 22$
$8 = 22^2 \bmod 97 = 484 \bmod 97 = 96$
$16 = 96^2 \bmod 97 = 9.216 \bmod 97 = 1$

Proses selanjutnya yaitu mengalikan hasil pangkat yang mempunyai nilai biner 1. Perhitungannya menjadi sebagai berikut:

$$\begin{aligned} 8^{21} \bmod 97 &= (8^1 * 8^4 * 8^{16}) \bmod 97 \\ &= (8 * 22 * 1) \bmod 97 \\ &= 176 \bmod 97 \\ &= 79 \end{aligned}$$

V. KESIMPULAN DAN SARAN

A. Kesimpulan

1) Algoritma ElGamal merupakan algoritma kunci asimetri dan kriptografi blok cipher. Hasil dari analisa proses enkripsi menghasilkan blok cipherteks dengan nilai a dan b yang diperoleh dari 1 (satu) karakter plainteks. Kelebihan dari blok cipher adalah karakter yang sama pada plainteks tidak akan menghasilkan karakter yang sama pada cipherteks. Sebagai contoh, "P" menjadi "El" dan "P" menjadi "q!".

2) Untuk membantu proses perhitungan perpangkatan dengan nilai besar dapat menggunakan perhitungan perpangkatan biner.

3) Dari uji coba yang dilakukan proses enkripsi dengan menggunakan kunci publik (63, 5, 97) untuk plainteks "PPKIA" menjadi blok cipherteks "El q! b= FD H1" dan kembali menjadi plainteks "PPKIA" dari proses dekripsi dengan menggunakan kunci privat (75, 97).

4) Tingkat keamanan algoritma ElGamal terlihat dari bagaimana pembentukan kunci publik dan privat terbentuk. Penentuan bilangan kunci yang sesuai dapat membuat pasangan kunci yang dapat digunakan untuk melakukan enkripsi dan dekripsi.

B. Saran

1) Untuk mengatasi pengamanan kata, bisa dilakukan dengan berbagai teknik selain kriptografi yaitu steganography. Dapat juga menggunakan kedua teknik yang ada yaitu kriptografi dan steganography, agar keamanan lebih maksimal.

2) Untuk nilai karakter dari plainteks dan cipherteks dapat menggunakan Tabel ASCII yang telah ada.

3) Analisa pengaman kata dapat dikembangkan dengan menggunakan metode-metode kriptografi lainnya yang seperti metode DES, RSA atau menggabungkan metode kriptografi lainnya agar bisa mendapatkan hasil yang maksimal.

4) Pada penelitian ini, penulis hanya sebatas melakukan analisa penerapan algoritma ElGamal terhadap kata tanpa membuat aplikasi sebagai pendukung dalam mengimplementasikan algoritma ElGamal.

UCAPAN TERIMA KASIH

Sehubungan dengan telah dirampungkannya penelitian mengenai analisa pengamanan kata dengan algoritma ElGamal, ijinkan penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada orang tua penulis, suami/istri, seluruh dosen serta rekan-rekan civitas akademika STMIK PPKIA Tarakanita Rahmawati dalam memberikan saran kepada penulis dan serta semangat sehingga penulis mampu menyelesaikan penelitian dengan tepat waktu. Terlepas dari ucapan terima kasih, penulis masih perlu masukan serta saran yang membangun demi penyempurnaan penelitian ini agar menjadi lebih baik lagi.

REFERENSI

[1] F.N. Pabokory, I.F. Astuti, and A.H. Kridalaksana, "Implementasi kriptografi pengamanan data pada pesan teks, isi file dokumen, dan file dokumen menggunakan algoritma advanced encryption standard," *Jurnal Informatika Mulawarman*, vol. 10, no. 1, pp. 20-31, Februari 2015.

[2] K. Nisak, "Penyandian kriptografi metode hill cipher dan caesar cipher dengan menggunakan appinventor," Skripsi, Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim: Malang, Juni 2015.

[3] Ratih, "Studi dan perbandingan penggunaan kriptografi kunci simetri dan asimetri pada telepon selular," Makalah, Program Studi Teknik Informatika Institut Teknologi Bandung: Bandung.

[4] D.T. Massandy, "Algoritma elgamal dalam pengamanan pesan rahasia," Makalah, Program Studi Teknik Informatika Institut Teknologi Bandung: Bandung.

[5] H. Kabetta, "Analisis kompleksitas waktu algoritma kriptografi elgamal dan data encryption standard," *Teknikom*, vol. 1, no.1, pp. 13-18, 2017.

[6] M. Rofiq and B.T.W Utomo, "Implementasi algoritma elgamal dalam sistem lock brankas berbasis mikrokontroler atmega16 dan smartphone android," *Jurnal Ilmiah Informatika*, vol. 1, no. 1, pp. 7-16, 2016.

[7] M.T. Tamam, W. Dwiono, and T. Hartanto, "Penerapan algoritma kriptografi elgamal untuk pengaman file citra," *Jurnal EECCIS*, vol. 4 no. 1, pp. 8-11, 2010.