PENGIRIMAN PESAN DENGAN ALGORITMA KRIPTOGRAFI ELGAMAL (Menggunakan Aplikasi Visual Basic)

Nur Fajrin Maulana Yusuf

Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Islam Makassar,
Jl. Perintis Kemerdekaan km.9 No. 29 Makassar, Indonesia 90245

nurfajrinmaulanayusuf@uim-makassar.ac.id

Abstract- **ElGamal merupakan algoritma kriptografi kunci asimetri. Keamanan algoritma ini terletak pada sulitnya memecahkan masalah logaritma diskrit. Penelitian ini diawali dengan konsep matematis yang melandasi pembentukan algoritma kriptografi ElGamal, tahap kedua adalah proses enkripsi, penandatanganan, dekripsi dan verifikasi pesan, tahap ketiga yaitu diterapkannya kriptografi ElGamal menggunakan bahasa pemrograman *Visual Basic*. Persamaan yang digunakan dalam algoritma kriptografi ElGamal adalah pembentukan kunci, dipilih bilangan prima p > 255, g < p, dan $x \in \{1, 2, \dots, p-2\}$. Nilai y diperoleh dengan persamaan $y_i = g_i^{xi}$ mod p_i, diperoleh kunci publik (*y,g,p*) dan kunci privat (*x,p*). Proses enkripsi dilakukan dengan memasukkan nilai $k_i \in \{1, 2, \dots, p_2 - 2\}$ pada persamaan $a_i = x_1^{ki} \ mod \ p_1$ dan $b_i = y_1^{ki} m_i \ mod \ p_1$, sehingga dihasilkan *Ciphertext* (a_i,b_i). Proses penandatanganan dilakukan dengan menghitung nilai *Hash*, kemudian pilih e$\in \{1, 2, \dots, p_1 - 2\}$ kedalam persamaan R=$g_1^e \ mod \ p_1$ dan T = (MD-xR)e^{-1} *mod* (p_1-1). Pesan dan tandatangan dikirim ke penerima kemudian didekripsi dengan persamaan $m_i = b_i(a_i^{x2})^{-1} \text{mod } p_2$. Pesan yang diperoleh penerima diverifikasi dengan memeriksa rentang nilai dan memenuhi persamaan $y_1{}^R R^T \equiv g_1{}^{MD} mod \ p_1$. Berdasarkan hasil penelitian diperoleh bahwa keamanan dalam proses pengiriman dan penerimaan pesan dapat ditingkatkan dengan algoritma kriptografi ElGamal dan tandatangan digital.**

Kata Kunci- ***Kriptografi ElGamal, Enkripsi, Dekripsi,Ciphertext, Plaintext***

I. PENDAHULUAN

Matematika sebagai ilmu pengetahuan dasar memegang peranan yang sangat penting dalam perkembangan ilmu pengetahuan lainnya, termasuk perkembangan teknologi informasi. Perkembangan teknologi informasi mempunyai pengaruh yang sangat signifikan bagi aspek kehidupan, tidak terkecuali aspek komunikasi dan pengiriman pesan. Dahulu pengiriman pesan hanya dilakukan di atas selembar kertas dan dikirim lewat kantor pos, tetapi kini pengiriman pesan telah berkembang seiring berkembangnya media telekomunikasi yang ada sekarang seperti *sms, fax, e-mail* maupun di media sosial yang berkembang pesat. Hal itu belum bisa menjamin persoalan yang penting pada pengiriman pesan tersebut.

Salah satu syarat untuk sebuah pesan ketika terkirim ke tujuan dengan kesahihan yang diperolehnya adalah keamanannya. Hal ini membuka banyak peluang adanya ancaman saat melintasi jaringan publik seperti internet yang diasumsikan dapat diakses oleh siapapun, termasuk orang-orang atau pihak-pihak yang memang berniat untuk menyadap, mencuri atau mengubah data untuk kepentingan tertentu.

Oleh karena itu, diperlukan suatu ilmu tertentu yang fokus mempelajari mengenai teknik-teknik penyandian suatu pesan dengan susunan algoritma-algoritma tertentu yang disebut kriptografi. Dalam proses kriptografi, pihak yang melakukan kegiatan terbagi menjadi dua bagian yaitu entitas pengirim (*sender*) dan entitas penerima (*receiver*) pesan. Dalam proses pengiriman dan penerimaan pesan juga terbagi menjadi dua proses, yaitu enkripsi (*encryption*) dan dekripsi (*decryption*). Enkripsi adalah proses penyandian/pengubahan pesan asli (*plaintext*) menjadi pesan rahasia (*chipertext*), sedangkan kebalikan dari proses enkripsi disebut

dekripsi. Proses enkripsi dan dekripsi tersebut menggunakan kunci dalam pengubahan pesan dengan menerapkan suatu algoritma.

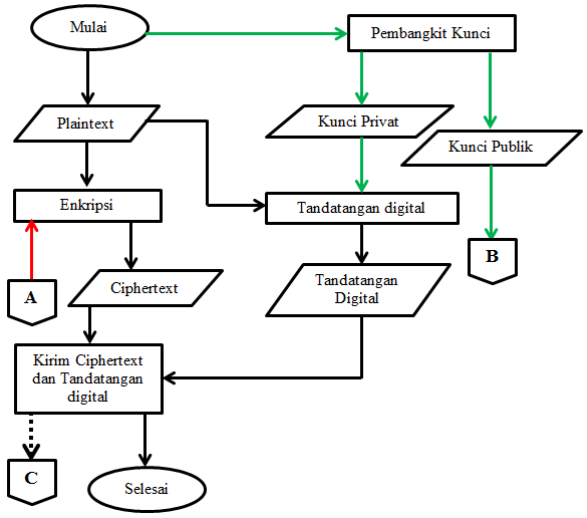
Algoritma kriptografi Elgamal dibuat oleh Taher ElGamal pada tahun 1984. Algoritma kriptografi ini pada umumnya digunakan untuk tandatangan digital, kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan deskripsi. Algoritma kriptografi ElGamal digunakan dalam perangkat lunak keamanan yang dikembangkan oleh GNU, program PGP, dan pada sistem keamanan lainnya. Kekuatan algoritma kriptografi ElGamal terletak pada sulitnya menghitung logaritma diskrit.

Penelitian mengenai kriptografi ElGamal telah banyak dilakukan oleh para kriptografer, antara lain Tamam, dkk. (2010) Penerapan Algoritma Kriptografi ElGamal Untuk Pengaman File Citra. Arizka (2011) Penerapan Sistem Kriptografi ElGamal atas Zp* dalam Pembuatan Tandatangan Digital. Singh dan Kumar (2012) *ElGamal's Algorithm in Cryptography*. Fujun (2013) *The Application of ElGamal Encryption Technology to the Information Security of Digital Library*. Oleh karena itu, penelitian ini akan membahas tentang salah satu konsep kriptografi dengan menggabungkan enkripsi berupa teks dan tandatangan digital, sehingga algoritma kriptografi ElGamal dapat diimplementasikan untuk kerahasiaan, autentikasi, keutuhan data dan bebas penyangkalan.

II. METODE PENELITIAN

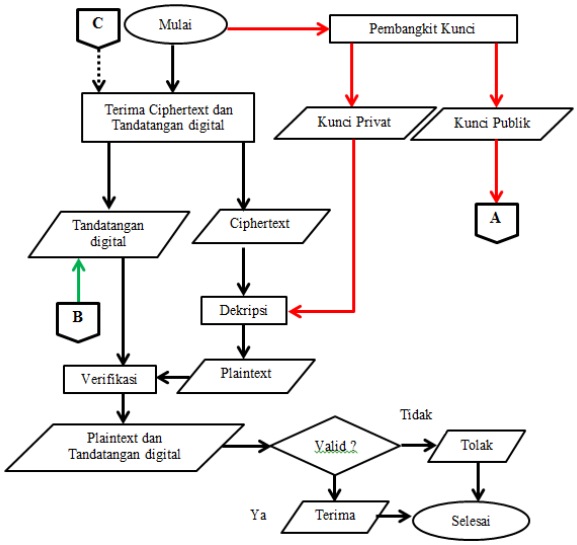
Penelitian yang digunakan yaitu studi literatur atau penelitian kajian kepustakaan dengan mengambil beberapa definisi, teorema, serta sifat-sifat yang berkaitan dengan penelitian

Prosedur penelitian yang akan diterapkan pada penelitian ini guna mencapai tujuan penelitian digambarkan pada gambar 1 dan Gambar 2.



Gambar 1. Diagram Alir Prosedur Penelitian Untuk Entitas Pengirim Pesan

Entitas pengirim pesan melakukan Enkripsi dengan kunci publik dari entitas penerima pesan yang menghasilkan *Ciphertext.* Disamping itu entitas pengirim pesan juga membangkitkan kunci, tandatangan digunakan dari kunci privat. Kunci publik dikirim ke entitas penerima pesan dengan *Ciphertext* dan tandatangan.



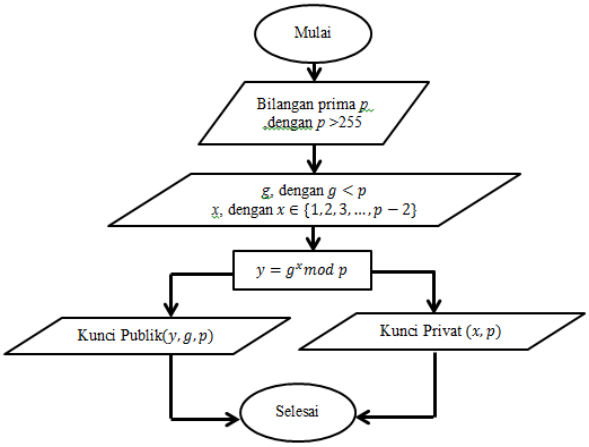
Gambar 2 Diagram Alir Prosedur Penelitian Untuk Entitas Penerima Pesan

Entitas penerima pesan menerima kunci publik, tandatangan dan *Ciphertext* dari entitas pengirim pesan. Sebelum itu entitas penerima pesan telah membangkitkan kunci, kunci privat digunakan untuk mendekripsikan *Ciphertext* ke *Plaintext*. Kunci Publik yang diterima dari entitas pengirim pesan dimasukkan ke dalam tandatangan kemudian diverifikasi keabsahan dari pesan tersebut.

Berdasarkan Gambar 1 dan Gambar 2, prosedur penelitian dapat dideskripsikan sebagai berikut :

1. Proses Pembangkitan Kunci

Pengirim dan penerima pesan tidak bisa melakukan enkripsi, dekripsi pesan, penandatanganan, dan verifikasi sebelum proses pembangkitan kunci terjadi. Proses pembangkitan kunci dilakukan oleh pengirim dan penerima dengan tujuan berbeda. Penerima pesan membangkitkan kunci untuk proses enkripsi dan dekripsi pesan. Sedangkan, pengirim pesan membangkitkan kunci untuk proses penandatangan dan verifikasi pesan.



Gambar 3. Diagram Alir Pembentukan Kunci

2. Enkripsi Pesan

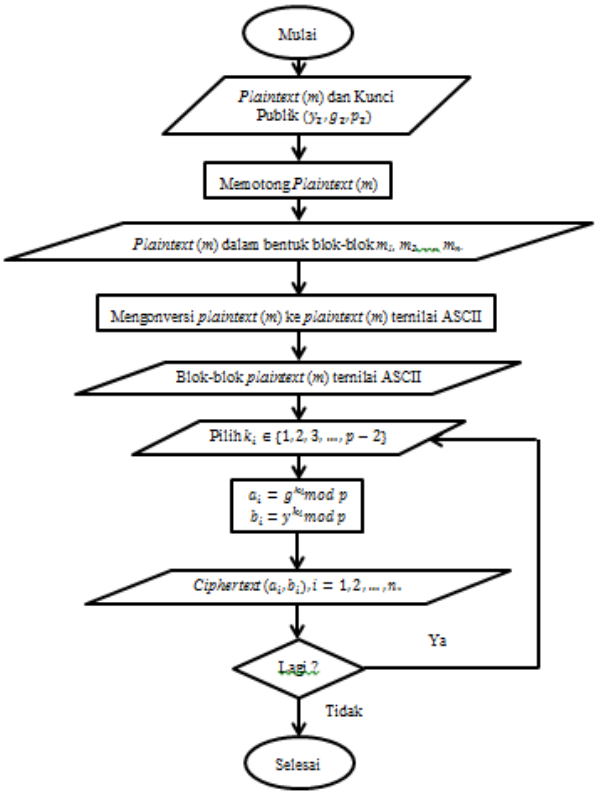
Pengirim pesan menuliskan *plaintext* (*m*) kemudian melakukan enkripsi pesan. Proses mengenkripsikan sebuah *plaintext* (*m*) membutuhkan kunci publik (y_2, g_2, p_2) yang sebelumnya telah dibuat oleh penerima pesan. Pengirim memilih sebarang bilangan bulat k dimana, $k \in 1, 2, 3, \dots, p_2 - 2\}$. Pesan yang akan disampaikan adalah *m*, kemudian dipecah tiap-tiap karakter yang dikonversi ke dalam Kode ASCII, sehingga *ciphertext* di atas menjadi *plaintext* $m_i \in \{1, 2, 3, \dots, p_2 - 1\}$, i = *1,2, ..,n.*. proses pengenkripsian yang dilakukan pada tiap-tiap blok *m* dapat dilihat pada persamaan (*1*) dan (*2*).

$$a_i = {g_2}^{k_i} mod\ p_2 \quad (1)$$

dan

$$b_i = {y_2}^{k_i} \cdot m \cdot mod\ p_2 \quad (2)$$

dengan $k_i \in \{1, 2, 3, \dots, p_2 - 2\}$ acak, sehingga nanti akan diperoleh *ciphertext* (a_i,b_i) untuk blok pesan *m*. jadi ukuran *ciphertext* dua kali ukuran *plaintext*.



Gambar 4. Diagram Alir Proses Enkripsi Pesan

3. Penandatanganan

Sebelum melakukan penandatangan terdapat sebuah fungsi yang digunakan untuk aplikasi keamanan, seperti otentifikasi dan integritas pesan. Fungsi tersebut ialah fungsi *hash*. Fungsi *hash* adalah fungsi yang menerima masukan string dengan masukannya dan mengonversikan menjadi string keluaran yang panjangnya tetap (Munir, R. 2006: 217). Jika string menyatakan pesan (*message*), maka pesan dimisalkan M yang ukurannya bebas, dimampatkan dengan fungsi hash melalui persamaan (3).

$$H(M) = MD \quad (3)$$

Dengan *MD* adalah nilai *hash* atau *message digest* dari fungsi *hash H* dengan masukan pesan *M*.

Proses penandatangan digital (*signing*) membutuhkan kunci privat dari pengirim dan juga nilai *hash* (*MD*) dari *plaintext* (*m*). Nilai *hash* yang dihasilkan adalah $MD \in \{1, 2, 3, \dots, p_1 - 2\}$. Kemudian memilih bilangan bulat *e* yang berada dalam {1, 2, 3, …, p_1 – 2} dan saling prima dengan $p_1 - 1$, dengan kata lain (e, $p_1 - 1$) = 1. Selanjutnya pengirim (*signer*) akan melakukan perhitungan sebagaimana pada persamaan (4) dan (5).

$$R = {g_1}^e mod\ p \quad (4)$$

dan

$$T = (MD - x_1 R)e^{-1} mod\ (p_1 - 1) \quad (5)$$

e^{-1} merupakan invers modulo dari e mod ($p_1 - 1$). Maka tandatangan pada dokumen tersebut adalah pasangan dari (R,T).

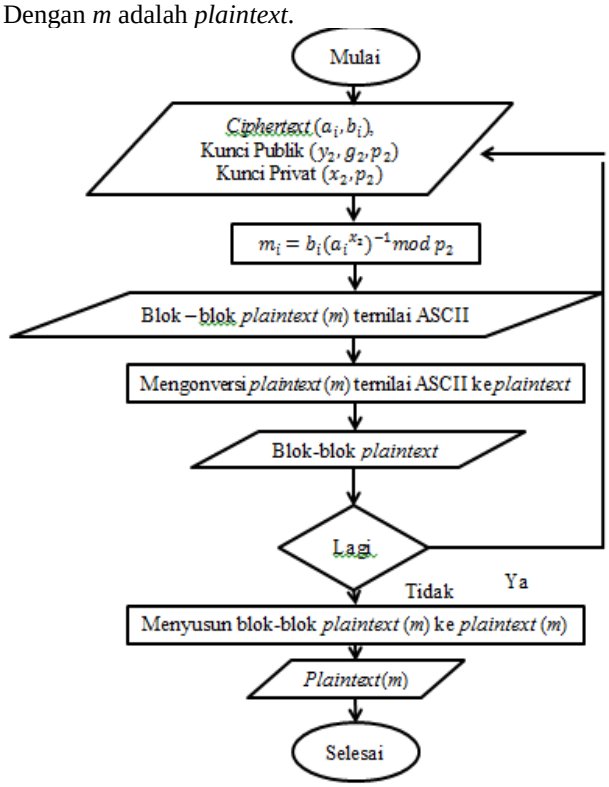
4. Dekripsi Pesan

Ciphertext beserta tandatangan digital telah terkirim ke penerima pesan. Maka penerima pesan akan mengubah *ciphertext* (a_i,b_i) menjadi *plaintext* (m). sehingga dapat dengan mudah membaca isi dari pesan tersebut. Untuk mendekripsi pesan, penerima pesan membutuhkan kunci privat (x_2, p_2).

Misalkan diberikan suatu kunci publik (y_2, g_2, p_2), dan kunci privat (x_2, p_2), serta *ciphertext* (a,b), maka *plaintext* (m) dapat diperoleh dengan menggunakan persamaan (6).

$$m_i = b_i(a_i{}^{x_2})^{-1} \, mod \, p_2 \qquad (6)$$

Dengan m adalah *plaintext*.



Gambar 5 Diagram Alir Proses Dekripsi Pesan

5. Verifikasi

Setelah pesan telah sampai kepada pihak penerima, maka penerima akan melakukan proses verifikasi. Untuk melakukan proses verifikasi, penerima pesan menggunakan kunci publik (y_1, g_1, p_1) yang telah diberikan dari pengirim pesan. Penerima memperoleh pesan berupa dokumen yang telah dibubuhi tandatangan digital. Sebelumnya, penerima mencari nilai *hash* dari dokumen yang diterima. Kemudian penerima akan memverifikasi tandatangan (R,T). Terlebih dahulu akan diperiksan apakah R memenuhi keberadaan {1, 2, 3, …, $p_1 - 1$}. Setelah memenuhi, dilanjutkan dengan mengecek apakah memenuhi persamaan (3.14).

$$y_1{}^R R^T \equiv g_1{}^{MD} mod\ p_1 \qquad (7)$$

Jadi verifikasi dikatakan berhasil jika memenuhi 2 keadaan berikut :

a. $1 \leq R \leq p_1 - 1$

b. Memenuhi persamaan (7)

Lalu akan ditunjukkan bahwa proses verifikasi telah bekerja. Jika T dihitung berdasarkan persamaan (3.12), maka

$$y_1{}^R R^T \equiv g_1{}^{x_1 R} g_1{}^{e(MD - x_1 R)e^{-1}} \equiv g_1{}^{MD} mod\ p_1 \qquad (8)$$

Sebaliknya jika (7) terpenuhi untuk pasangan tandatangan (R,T) dan jika e adalah logaritma diskrit dari R dengan basis g_1, atau bisa ditulis dengan $R = g_1{}^e$, maka

$$y_1{}^R R^T \equiv g_1{}^{x_1 R} g_1{}^{eT} \equiv g_1{}^{x_1 R + eT} \equiv g_1{}^{MD} mod\ p_1 \qquad (9)$$

g adalah bilangan bulat bermodulo p, mengakibatkan

$$x_1 R + eT \equiv MD \ mod\ (p_1 - 1) \qquad (10)$$

III. HASIL PENELITIAN

1. Konsep Matematis

Algoritma kriptografi ElGamal didasarkan pada sulitnya menghitung logaritma diskrit. Logaritma diskrit merupakan invers dari eksponensial diskrit dalam grup siklik terhingga, sehingga menghasilkan konsep matematis untuk sistem algoritma kriptografi ElGamal.

Sistem algoritma kriptografi ElGamal yang tumpuan matematisnya terletak pada masalah logaritma diskrit. Proses pada sistem algoritma kriptografi ElGamal dapat dijelaskan sebagai berikut:

a. Pembentukan Kunci

1) Pilih bilangan prima $p > 255$
2) Pilih bilangan bulat $g < p$
3) Pilih bilangan bulat x yang memenuhi $1 \leq x \leq p - 2$
4) Hitung
$$y = g^x mod\ p \qquad (11)$$
5) Kunci publik (y, g, p) dan kunci privat (x,p)

b. Proses Enkripsi

1) Konversi blok-blok *plaintext* (m_i) ke *plaintext* (m_i) ternilai ASCII. $i \in \{1, 2, \ldots, n\}$. n adalah banyaknya karakter dalam pesan.
2) Pilih $k_i \in \{1, 2, \ldots, p_2 - 1\}$
3) Hitung
$$a_i = g_2{}^{k_i} mod\ p_2 \qquad (12)$$
4) Hitung
$$b_i = y_2{}^{k_i}.m_i \ mod\ p_2 \qquad (13)$$
5) *Ciphertext* (a_i, b_i)

c. Proses Dekripsi

1) Hitung
$$m_i = b_i(a_i{}^{x_2})^{-1} mod\ p_2 \qquad (14)$$

Pesan dibuktikan dengan subtitusi persamaan (12) dan (13) ke persamaan (14) maka menghasilkan persamaan (15).

$$m_i = {y_2}^{k_i}.m_i.(({g_2}^{k_i})^{x_2})^{-1} mod\ p_2 \quad (15)$$

Kemudian Subtitusi persamaan (11) ke persamaan (1) maka menghasilkan persamaan (16)

$$m_i = ({g_2}^{x_2})^{k_i}.m_i.(({g_2}^{k_i})^{x_2})^{-1} mod\ p_2$$
$$m_i = m_i.({g_2}^{x_2 k_i}).({g_2}^{x_2 k_i})^{-1} mod\ p_2$$
$$m_i = m_i\ mod\ p_2 \quad (16)$$

d. Proses Pembuatan Tandatangan

1) Hitung $MD = H(M)$, $MD \in \{1, 2, 3, \dots, p_1 - 2\}$

2) Pilih $e \in \{1, 2, 3, \dots, p_1 - 2\}$ yang relatif prima dengan $p_1 - 1$

3) Hitung

$$R = {g_1}^{e} mod\ p_1 \quad (17)$$
$$T = (MD - x_1 R)e^{-1} mod\ (p_1 - 1) \quad (18)$$

4) Tandatangan (R,T)

e. Proses Verifikasi

1) Memenuhi $1 \le R \le p_1 - 1$

2) Hitung

$${y_1}^{R} R^T \equiv {g^{MD}}(mod\ p_1) \quad (19)$$

Tandatangan dibuktikan dengan subtitusi persamaan (11), (17) dan (18) ke persamaan (19) maka akan menghasilkan persamaan (20).

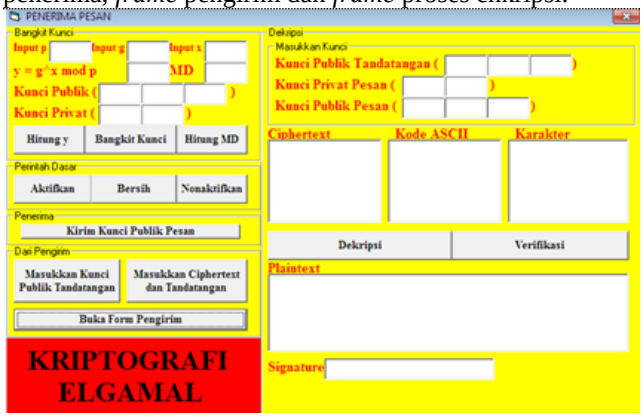
$${y_1}^{R} R^T \equiv {g_1}^{x_1 g_1^{\ e}} {g_1}^{e(MD - x_1 g_1^{\ e})e^{-1}} \equiv {g_1}^{MD}(mod\ p_1)$$
$${y_1}^{R} R^T \equiv {g_1}^{x_1 g_1^{\ e} + e(MD - x_1 g_1^{\ e})e^{-1}} \equiv {g_1}^{MD}(mod\ p_1)$$
$${g_1}^{x_1 g_1^{\ e} + MD - x_1 g_1^{\ e}} \equiv {g_1}^{MD}(mod\ p_1)$$
$${g_1}^{MD} \equiv {g_1}^{MD}(mod\ p_1) \quad (20)$$

2. Implementasian Kriptografi ElGamal dengan Bahasa Pemrograman Visual Basic

Implementasi ini dilakukan dengan membuat sebuah program, yang dapat melakukan enkripsi, dekripsi, penandatanganan dan verifikasi pesan. Adapun contoh form sebagai berikut :

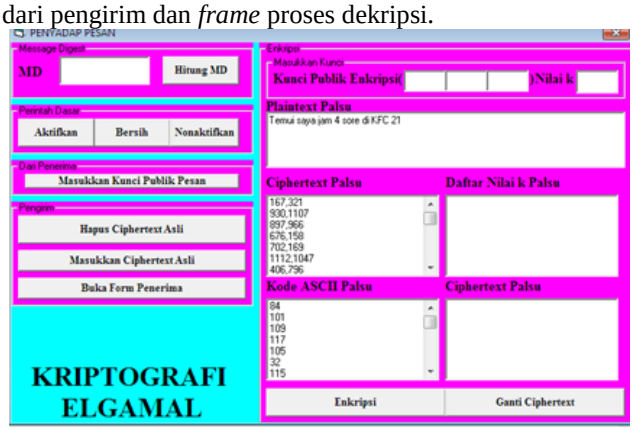
Gambar 6 Tampilan *Form* Pengirim Pesan

Gambar 6. merupakan tampilan dasar dari *form* pengirim pesan yang terdiri dari beberapa *frame*. *Frame* tersebut memuat beberapa bagian dalam proses pengiriman pesan yaitu *frame* bangkit kunci tandatangan, *frame* perintah dasar, *frame* dari penerima, *frame* pengirim dan *frame* proses enkripsi.



Gambar 7. Tampilan Form Penerima Pesan

Gambar 7. merupakan tampilan dasar dari *form* penerima pesan yang terdiri dari beberapa *frame*. *Frame* tersebut memuat beberapa bagian dalam proses penerimaan pesan yaitu *frame* bangkit kunci, *frame* perintah dasar, *frame* penerima, *frame* dari pengirim dan *frame* proses dekripsi.



Gambar 8. Tampilan Form Proses Penyadapan Pesan

Gambar 8. merupakan tampilan dasar dari *form* Proses penyadapan pesan yang terdiri dari beberapa *frame*.

3. Perumusan Algoritma Kriptografi ElGamal

Algoritma kriptografi ElGamal didasarkan pada logaritma diskrit pada grup siklik terhingga yang dikongruenkan. Sehingga menghasilkan rumus enkripsi dan dekripsi yang saling berkaitan. *Plaintext* yang dienkripsikan dengan kunci publik menghasilkan *ciphertext* dan selanjutnya didekripsikan dengan kunci privat akan menghasilkan *plaintext* kembali. Bukan hanya proses enkripsi dan dekripsi bahkan proses penandatanganan dan verifikasi menggunakan masalah logaritma diskrit.

4. Proses Enkripsi, Proses Dekripsi, Proses Pembuatan Tanda Tangan, dan Proses Verifikasi Algoritma Kriptografi ElGamal

Algoritma kriptografi ElGamal terdiri dari dua buah kunci yaitu kunci publik dan kunci privat. Keuntungan menggunakan algoritma kriptografi kunci publik adalah tidak ada permasalahan pada distribusi kunci apabila jumlah pengirim sangat banyak serta tidak ada kepastian keamanan jalur yang digunakan.

Proses pembentukan kunci dilakukan oleh pengirim dan penerima pesan, tetapi diterapkan pada proses yang berbeda. Pengirim pesan melakukan pembentukan kunci untuk proses penandatanganan dan proses verfikasi yang nantinya kunci publik akan diserahkan ke penerima pesan dan kunci privat akan dirahasiakan. Sedangkan, penerima pesan melakukan pembentukan kunci untuk proses enkripsi dan proses dekripsi pesan yang nantinya kunci publik akan diserahkan ke pengirim dan kunci privat akan dirahasiakan.

Kunci publik dapat diketahui secara umum. Namun, dengan menyisipkan tandatangan digital pada pesan memungkinkan penerima pesan dapat mengetahui pengirim pesan sehingga dapat mengantisipasi pesan yan tidak diharapkan.

Penelitian ini dilakukan dengan simulasi pesan yang utuh serta dikirim oleh pengirim sebenarnya dan pesan yang telah mengalami pengubahan dalam hal ini adalah *ciphertext* sedang tandatangan digital masih milik pengirim asli. Pengirim pesan adalah entitas pengirim pesan dalam hal ini pengenkripsi dan pembuat tandatangan digital, sedangkan penerima pesan adalah entitas penerima pesan dalam hal ini pendekripsi dan pemeriksa verifikasi terhadap tandatangan digital.

IV. KESIMPULAN DAN SARAN

A. KESIMPULAN

Berdasarkan hasil penelitian, maka diperoleh kesimpulan sebagai berikut :

1. Konsep matematis yang melandasi terbentuknya algoritma kriptografi ElGamal adalah masalah logaritma diskrit, misalkan G adalah suatu grup siklik dengan order *n*, a adalah pembangun G dan elemen identitas dari G adalah 1. Diberikan $y \epsilon$ G. Masalah yang dimunculkan ialah bagaimana menentukan suatu bilangan bulat nonnegatif terkecil b sedemikian sehingga $y \equiv a^b$. Perhitungan proses pembentukan kunci $y = g^x mod\ p$, enkripsi $a_i = {g_2}^{k_i} mod\ p_2$ dan $b_i = {y_2}^{k_i} m_i mod\ p_2$, penandatangan $R = {g_1}^e mod\ p_1$, dekripsi $m_i = b_i({a_i}^{x_2})^{-1} mod\ p_2$, serta verifikasi ${y_1}^R R^T \equiv g^{MD} (mod\ p_1)$ yang berdasar pada logaritma diskrit.
2. Proses Enkripsi algoritma kriptografi ElGamal pada pengiriman pesan yaitu 1) *Plaintext* dipotong menjadi blok-blok karakter; 2) Konversi ke Kode ASCII; 3) Gunakan rumus enkripsi.
3. Proses pembuatan tandatangan digital menggunakan algoritma kriptografi ElGamal pada pengiriman pesan yaitu 1) Hitung *MD* ;2) Gunakan rumus *signing.*
4. Proses Dekripsi algoritma kriptografi ElGamal pada pengiriman pesan yaitu 1) Gunakan rumus dekripsi; 2) Konversi nilai terkode ASCII ke teks karakter; 3) Gabungkan menjadi *plaintext.*
5. Proses Verifikasi tandatangan digital menggunakan algoritma kriptografi ElGamal pada pengiriman pesan yaitu 1) Nilai R terdapat pada rentang nilai $1 \leq R \leq p_1 - 1$; 2) Memenuhi rumus verifikasi.

B. SARAN

Adapun saran yang diajukan penulis adalah sebagai berikut :

1. Diharapkan kepada pembaca ataupun peneliti selanjutnya untuk dapat mengkaji lebih jauh tentang *plaintext* algoritma kriptografi ElGamal yang berupa *file* data, *image* (citra), video, audio, dan sebagainya.
2. Diharapkan kepada pembaca ataupun peneliti selanjutnya untuk dapat mengkaji lebih jauh proses perhitungan nilai *hash* yang aman dari *collision*.
3. Diharapkan kepada pembaca ataupun peneliti selanjutnya untuk dapat mengkaji lebih jauh kombinasi algoritma kriptografi ElGamal dengan algoritma kriptografi lainnya.
4. Algoritma kriptografi ElGamal diimplementasikan menggunakan bahasa pemrograman lain, seperti C/C++, PHP, Java, Matlab, Turbo Pascal, dan sebagainya.

DAFTAR PUSTAKA

Ariyus, D. 2009. *Keamanan Multimedia*. Yogyakarta: Penerbit Andi.

Arizka, R.U. 2011 *Penerapan Sistem Kriptografi ElGamal Atas Zp* Dalam Pembuatan Tanda Tangan Digital*. Yogyakarta: Universitas Negeri Yogyakarta.

Fujun, Z. 2013. *The Application of ElGamal Encryption Technology to the Information Security of Digital Library*. Jurnal TELKOMNIKA. Vol. 11, No. 12, http://download.portalgaruda.org/article.php?article=100418&val=160

Jubilee Enterprise. 2013. *Visual Basic 2013 Untuk Pemula*. Bandung : Elex Media Computindo.

Kromodimoeljo, S. 2009. *Teori dan Aplikasi Kriptografi*. SPK IT *Consulting*. *E-Book.*

Munir, R. 2006. *Kriptografi*. Bandung: Informatika Bandung.

Munir, R. 2012. *Matematika Diskrit (Edisi Revisi Kelima)*. Bandung: Informatika Bandung.

Sadikin, R. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: Penerbit Andi.

Singh, R., dan Kumar, S., 2012. *ElGamal's Algorithm in Cryptography*. International Journal of Scientific & Engineering Research, Vol. 3, Issue 12, www.ijser.org/ researchpaper /CElgamals-Algorithm-in-Cryptography.pdf,

Suhan, N. 2013. *Penerapan Algoritma Kriptografi RSA Pada Pengiriman Pesan Rahasia*. Makassar: Universitas Negeri Makassar.

Tamam, M.T., Dwiono, W., Hartanto, T. 2010. *Penerapan Algoritma Kriptografi ElGamal untuk Pengaman File Citra*. Jurnal *Electrical Power Electronic Communication Control Information Seminar (EECCIS),* Vol. VI, No. 1,jurnaleeccis.ub.ac.id/index.php/eeccis/article /view/95/94

Tiro, M.A., Darwis, M., Sukarna, Aswi. 2008. *Pengenalan Teori Bilangan*. Makassar: Andira *Publisher*.

WAHANA KOMPUTER. 2013. *Paling Dicari Visual Basic 2012 Source Code*. Yogyakarta : Penerbit Andi

Zelvina, A., Efendi, S., Arisandi, D. 2012. *Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa*. Jurnal DUNIA TEKNOLOGI INFORMASI, Vol. 1, No. 1, http://download.portalgaruda.org/article.php?article=58999&val=4123