ENKRIPSI EMAIL DENGAN MENGGUNAKAN METODE ELGAMAL PADA PERANGKAT MOBILE

Yudhistira Taufan A.[1], Idris Winarno, S.ST., M.Kom[2], Kholid Fathoni, S.Kom.[2]
Mahasiswa[1] , Dosen [2]
Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember
Kampus PENS-ITS Keputih Sukolilo Surabaya 60111
Telp (+62)31-5947280, 5946114, Fax. (+62)31-5946114

Abstrak

Pada proyek akhir ini dibuat sebuah enkripsi yang diintegrasikan dengan aplikasi email client yang sudah ada untuk menambah keamanan pada proses pengiriman email pada perangkat mobile tersebut. Dengan menggunakan metode enkripsi ElGamal, diharapkan proses pengiriman email yang dilakukan melalui perangkat mobile menjadi lebih secure. Karena, adanya public key dan private key yang hanya diketahui oleh pengirim dan penerima pesan. Output yang dihasilkan merupakan cipherteks yang mana ketika penerima ingin membacanya, perlu untuk melakukan proses dekripsi. Selain itu, proses enkripsi pada plainteks yang sama diperoleh cipherteks yang berbeda-beda, namun pada proses dekripsi diperoleh plainteks yang sama. Sehingga, membuat email menjadi lebih secure dibanding sebelumnya.

Kata Kunci : mobile, email, ElGamal, secure, public key, private key, cipherteks

1. Pendahuluan

1.1 Latar Belakang

Email sudah digunakan orang sejak awal terbentuknya internet dan merupakan salah satu fasilitas yang ada pada saat itu. Tak jarang orang menyimpan berbagai data penting pada email tersebut. Sepeti informasi akun - akun, nomor rekening relasi, dan masih banyak lainnya. Hal ini di-karenakan orang - orang takut lupa mengenai informasi penting tersebut dan dipili-hlah email sebagai tempat penyimpanannya.

Namun, akibat dari banyaknya orang yang menggunakan email tersebut sebagai alat penyimpan informasi, tak sedikit orang yang berbuat nakal untuk mencari tahu mengenai informasi tersebut. Salah satu caranya adalah dengan melakukan hack ke email sang korban.

Permasalahan tersebut dapat diatasi dengan proses enkripsi. Salah satu enkripsi yang cukup dikenal adalah dengan metode enkripsi ElGamal. ElGamal ini akan memberikan public key serta private key yang digunakan dalam proses Enkripsi dan Dekripsi. Dalam proses pembentukan kunci public dan rahasia, akan dibutuhkan suatu bilangan prima yang bernilai besar agar menjadi aman. Aplikasi enkripsi email ini akan dibangun pada perangkat mobile berbasis Android. Sehingga diharapkan akan dapat memproteksi masyarakat yang mengirimkan email menggunakan perangkat mobile.

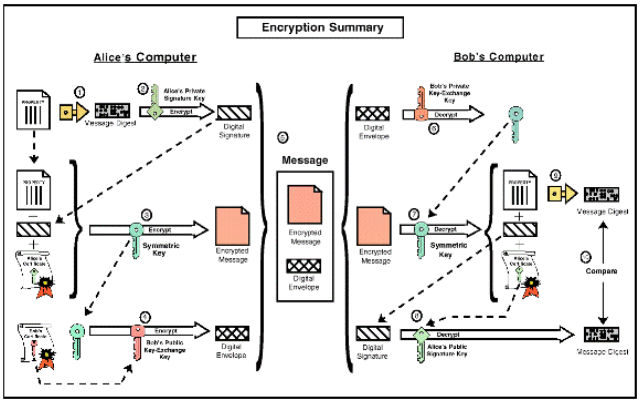
Rumusan masalah dari aplikasi ini adalah Mengintegrasikan metode enkripsi Elgamal ini dengan aplikasi mobile email client berbasis Android, embangkitkan bilangan acak (prima dan tidak prima) untuk menjadi kunci dalam sistem kriptografi, mengonversi karakter plainteks ke chiperteks atau sebaliknya dengan menggunakan tabel ASCII, dimana jumlah maksimal karakter ASCII harus bilangan prima, menghasilkan output yang secure, yaitu berupa kode-kode hasil enkripsi dari email yang akan dikirimkan.

Tujuan dari aplikasi ini adalah menghasilkan pasangan kunci yang berguna dalam proses kriptografi Elgamal. Pasangan kunci yang dihasilkan merupakan kunci publik dan kunci privat, memroses suatu kunci publik yang memiliki tiga buah bilangan, yaitu (y, g, p). Dimana y merupakan kunci publik yang didapatkan dari fungsi y = gx mod p, g merupakan bilangan acak, dan p merupakan bilangan prima, memroses suatu kunci privat berdasarkan password yang diinputkan dari user, menghasilkan suatu chipertext yang memiliki panjang dua kali lebih banyak dari plaintext awal, mendapatkan suatu plaintext awal berdasarkan chipertext yang telah dilakukan enkripsi.

2. Teori Penunjang

Kriptografi menjadi dasar bagi keamanan komputer dan jaringan karena yang menjadi pokok dari fungsi komputer dan jaringan adalah data ataupun informasi. Komputer dan jaringannya menjadi sarana bagi distribusi data dan informasi, maka data dan informasi tersebut harus diamankan

agar hanya orang-orang yang berhak mengaksesnya yang dapat mengetahui maupun menggunakan data tersebut. Salah satu cara yang paling banyak digunakan dalam mengamankan data adalah dengan kriptografi.



Gambar 2.1. Gambaran Umum Kriptografi

Proses Enkripsi

Langkah proses enkripsi: Proses enkripsi menggunakan kunci publik (p,g,y) dan sebuah bilangan integer acak k (k ∈{0,1,..., p − 1}) yang dijaga kerahasiaannya oleh penerima 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 (a,b).

a) Ambil sebuah karakter dalam pesan yang akan dienkripsi dan transformasi karakter tersebut ke dalam kode ASCII sehingga diperoleh bilangan bulat m. Plainteks tersebut disusun menjadi blok-blok m1, m2, ……, sedemikian hingga setiap blok merepresentasikan nilai di dalam rentang 0 (nol) sampai p-1.
b) Memilih bilangan acak k, yang dalam hal ini 0 < k < p-1, sedemikian hingga k relative prima dengan p-1.
c) Hitung nilai a dan b dengan persamaan berikut :
   $a = g^k \pmod p$ ……(4)
   $b = y^k m \pmod p$ ……..(5)
d) Diperoleh cipherteks untuk karakter m tersebut dalam blok (a,b)
e) Melakukan proses di atas untuk seluruh karakter dalam pesan termasuk karakter spasi.

Proses Dekripsi

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

Teorema :

Diberikan (p,g,y) sebagai kunci public dan x sebagai kunci rahasia pada algoritma ElGamal. Jika diberikan cipherteks (a, b), maka

$m = b/a^x \pmod p$ ..... (4)

dengan M adalah plainteks.

Di mana nilai

$(ax)^{-1} = r^{-a} = rp^{-1-a} \pmod p$. … (5)

Langkah proses dekripsi:

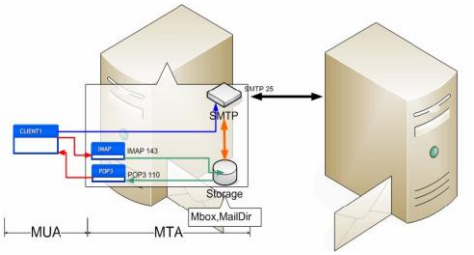
a. Ambil sebuah blok cipherteks dari pesan yang telah dienkripsikan pengirim.
b. Dengan menggunakan a yang dirahasiakan oleh penerima, hitung nilai plainteks dengan menggunakan "persamaan (4)" dan "persamaan (5)".

EMAIL (Electronic Mail)

Electronic-Mail (E-Mail) merupakan aplikasi TCP/IP yang paling banyak di-gunakan. E-mail adalah pesan yang terdiri atas kumpulan string ASCII dalam format RFC 822 (dikembangkan thn 1982).

Cara Kerja Email

Berikut ini adalah gambaran dari cara kerja email :



Gambar 2.4. *Cara Kerja Email*

Cara kerja email dapat dilihat pada Gambar 6.1. E-mail yang dikirim be-lum tentu akan diteruskan ke komputer penerima (end user), tapi disim-pan/dikumpulkan dahulu dalam sebuah komputer server (host) yang akan online secara terus menerus (continue) dengan media penyimpanan (storage) yang relatif lebih besar dibanding komputer biasa. Hal ini bisa diibaratkan dengan sebuah kan-tor pos, jika sesorang mempunyai alamat (mailbox), maka dia dapat memeriksa secara berkala jika dia mendapatkan surat. Komputer yang melayani penerimaan email

secara terus-menerus tersebut biasa disebut dengan mailserver atau mailhost.

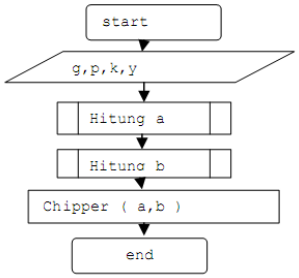
SSL

Secure Socket Layer (SSL) adalah protokol yang digunakan untuk browsing web secara aman. SSL bertindak sebagai protokol yang mengamankan komunikasi antara client dan server. Protokol ini memfasilitasi penggunaan enkripsi untuk data yang rahasia dan membantu menjamin integritas informasi yang dipertukarkan antara website dan web browser. SSL dikembangkan oleh Netscape Communations pada tahun 1994.

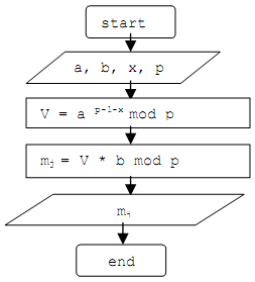
Selain itu SSL adalah Protokol berlapis. Dalam tiap lapisannya, sebuah data terdiri dari panjang, deskripsi dan isi. SSL mengambil data untuk dikirimkan, dipecahkan kedalam blok-blok yang teratur, kemudian dikompres jika perlu, menerapkan MAC, dienkripsi, dan hasilnya dikirimkan. Di tempat tujuan, data didekripsi, verifikasi, dekompres, dan disusun kembali. Hasilnya dikirimkan ke klien di atasnya.

3. Rancangan Sistem

3.1 Metode Elgamal sebagai alat untuk enkripsi



Gambar 2.4. *Flowchart Enkripsi*



Gambar 2.4. *Flowchart Dekripsi*

Proses pada project akhir ini adalah :

1) Proses pembangkitan bilangan pemicu → Proses tersebut adalah proses untuk membangkitkan bilangan acak prima sebagai pemicu terhadap kunci kunci ElGamal sehingga menambah kerumitan dalam penghitungannya. Semakin rumit penghitungan maka akan semakin aman algoritma tersebut.
2) Pembangkitan kunci privat (x) → yaitu proses untuk menghitung bilangan x dari kata kunci (dalam frase atau kalimat) yang dinputkan user. Dengan proses ini maka x tidak akan keluar dari range yang ditentukan dalam ElGamal.
3) Pembangkitan kunci publik (y) → proses ini adalah menghitung kunci publik (y) dengan menggunakan kunci privat (x). Tujuannya adalah kunci y tersebut yang akan di sebarkan kepada publik, sehingga orang lain dapat meng-enkripsi pesan yang akan dikirim pada kita. Dan kita dapat mendekripsi pesan tersebut dengan kunci x(privat).
4) Enkripsi pesan → proses yang digunakan untuk menyandikan plain text atau pesan email awal. Dengan metode ElGamal maka proses ini akan menghasilkan chipertext (sandi) dengan 2 karakter mewakili 1 karakter plaintext. Jadi chipertext dua kali jumlahnya dari plaintext.
5) Mengirim pesan → proses ini adalah proses mengirim pesan dengan Java mail ke EMail Server. Proses ini menggunakan protokol SMTP untuk mengirim email tersebut. Pesan yang dikirim berupa byte[] sehingga proses pengiriman dapat berjalan lancar dan dapat diterima oleh Mail Server.
6) Membaca email → proses ini adalah proses untuk membaca email yang dikirim. Awalnya Email Client melakukan download pesan pada Mail Server dengan menggunakan protokol POP3 atau Imap. User dapat memilih salah satu dari 2 protokol tersebut. Setelah melakukan download maka pesan ditampilkan di table pesan.
7) Dekripsi email → pesan di eMail Server tidak di dekripsi. Selalu dalam chipertext. Jadi untuk membaca email dilakukan proses dekripsi terlebih dahulu. Proses ini melakukan pengecekan kunci privat terlebih dahulu. Kemudian proses dekripsi dapat dilakukan dengan menghasilkan plaintext yang sama ketika sebelum di enkripsi oleh pengirim email.

4. Uji Coba dan Analisa

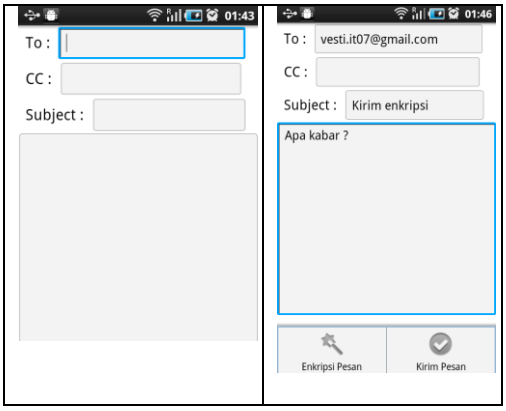
4.1 Uji Coba Proses Enkrip Email

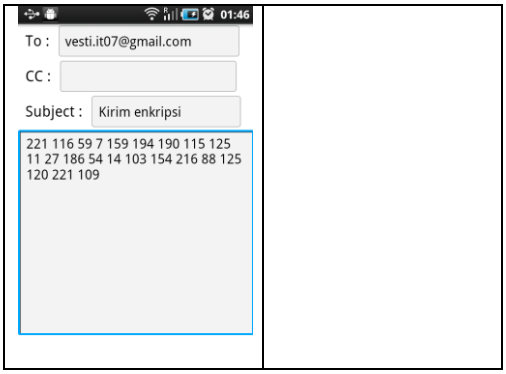
Tujuan dari uji coba ini adalah untuk memastikan proses enkripsi telah berjalan dengan

baik dan siap untuk dilakukan proses pengiriman message.

Tabel 4. 1 Tabel Uji Coba Proses Enkripsi

Kode Uji Coba		UC-04	
Use Case		Encrypt Email	
Tujuan		Melakukan uji coba fungsio-nalitas enkripsi dengan metode Elgamal	
Precondition		*User* berada pada menu Kirim Email untuk memilih menu Enkripsi.	
No	**Input**	**Hasil yang diharapkan**	**Hasil Akhir**
1.	*User* memasukkan *email* yang ingin dikirimkan	Menampilkan inputan tujuan yang dilakukan oleh *user*.	Ok
2.	*User* memasukkan kunci publik digunakan untuk melakukan enkripsi	Hasil enkripsi akan ditampilkan setelah dilakukan proses terhadap kunci publik	Ok
Post Condition		Menampilkan hasil enkripsi pada *content message*.	





Gambar 4.4 Proses *Encrypt Message*

Analisa :

Proses *Encrypt Message* yang dilakukan ini akan berjalan ketika *Public Key* telah diinputkan. Kemudian, email yang telah ditulis akan dilakukan proses enkripsi. Proses enkripsi ini akan menghasilkan 2 variable, yaitu kodechiper dan kodechipangka.

Kodechiper merupakan suatu chipertext hasil enkripsi dari suatu plainteks . Sedangkan kodechipangka merupakan suatu bilangan hasil enkripsi pesan. Kodechipangka ini berguna ketika dilakukan pengiriman, karena suatu mail server tidak mengenali karakter – karakter pada kodechiper, sehingga ketika melakukan proses pengiriman, yang dikirim adalah kodechipangka

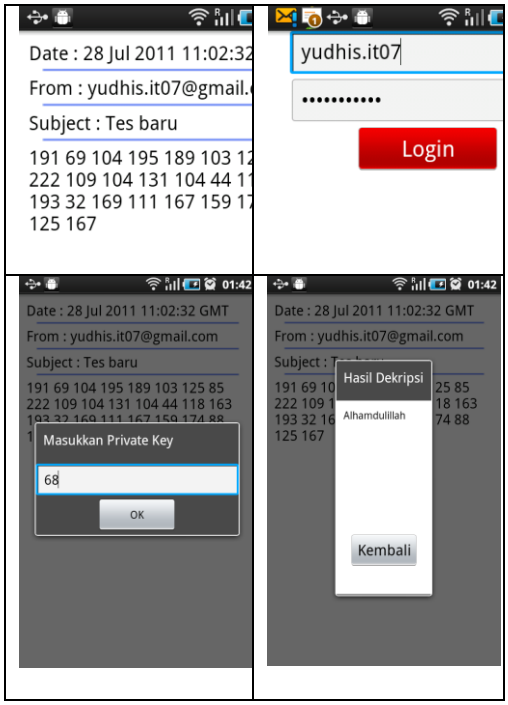
4.2 Uji Coba Proses Dekrip Email

Tujuan dari uji coba ini adalah untuk memastikan proses dekripsi telah berjalan dengan baik sehingga *user* dapat membaca *email* yang telah dienkripsi.

Tabel 4. 5 Tabel Uji Coba Proses Dekripsi

Kode Uji Coba		UC-05	
Use Case		Decrypt Email	
Tujuan		Melakukan uji coba fungsio-nalitas dekripsi dengan metode Elgamal	
Precondition		*User* berada pada menu Lihat *Email* untuk memilih isi dari pesan.	
No	**Input**	**Hasil yang diharapkan**	**Hasil Akhir**
1.	*User* membuka *email* yang telah	Menampilkan iinformasi dari suatu *message*	Ok

	dilakukan enkripsi		
2.	*User* memasukkan kunci privat digunakan untuk melakukan dekripsi	Hasil dekripsi akan ditampilkan setelah dilakukan proses terhadap kunci privat	Ok
Post Condition		Menampilkan hasil dekripsi pada *content message*.	



Gambar 4.2 Proses *Decrypt Message*

Analisa :

Proses *Decrypt Message* yang dilakukan ini akan berjalan ketika *Private Key* telah diinputkan. Kemudian, akan mengambil email yang telah dienkripsi dan selanjutnya akan dilakukan proses dekripsi. Proses dekripsi ini tidak akan berjalan dengan baik apabila *private key* yang diinputkan tidak sesuai dengan pasangan kunci publiknya.

Kodechiper merupakan suatu chipertext hasil enkripsi dari suatu plainteks . Sedangkan kodechipangka merupakan suatu bilangan hasil enkripsi pesan. Kodechipangka ini berguna ketika dilakukan pengiriman, karena suatu mail server tidak mengenali karakter – karakter pada kodechiper, sehingga ketika melakukan proses pengiriman, yang dikirim adalah kodechipangka

5. Kesimpulan

- Penerapan Algoritma Kriptografi *Elgamal* pada sistem yang dibuat telah sesuai dengan proses algoritma Kriptografi *Elgamal* yang ada. Hal ini dibuktikan dengan terbentuknya pasangan kunci publik dan kunci privat.
- Kunci Publik yang dihasilkan, memiliki tiga buah bilangan yang terdiri dari nilai y, g, dan p. Nilai p yang baik adalah bilangan prima terbesar berdasarkan nilai ASCII dimana dalam proyek akhir ini bernilai 223. Kemudian nilai g merupakan suatu nilai bilangan konstanta yang diinisialisasikan dengan nilai 13. Kemudian, nilai y didapat dengan fungsi $\mathbf{y = g^x \bmod p}$, dimana nilai x merupakan variabel kunci privat.
- Proses yang dilakukan untuk mencari kunci privat berdasarkan suatu inputan dari *user*, telah dapat dihasilkan yang dapat digunakan pada proses pencarian kunci publik.
- Hasil enkripsi yang dihasilkan memiliki panjang dua kali lipat dari panjang *plaintext* awal. Hal ini dikarenakan setiap blok *plaintext* dienkripsi dengan mencari pasangan *chipertext* $\mathbf{a = g^k \bmod p}$ dan $\mathbf{b = y^k m \bmod p}$. Sehingga, setiap blok pesan M akan menghasilkan pasangan (a,b). Jadi, ukuran *chipertext* yang dihasilkan adalah dua kali ukuran *plaintext*.
- Dalam membaca hasil enkripsi yang telah dikirimkan, maka dilakukan dekripsi berdasarkan pasangan (a,b). Maka fungsi yang digunakan dalam proses dekripsi dengan menggunakan rumus $\mathbf{M = b/a^x \bmod p}$. **M** merupakan hasil *plaintext* yang didapatkan sesuai dengan *plaintext* sebelum dilakukan enkripsi.

DAFTAR PUSTAKA

[1.] Munir, Rinaldi, 2005. "*Algoritma ElGamal "*,STEI – ITB

[2.]*http://id.wikipedia.org/wiki/Android_%28sistem_ operasi%29*
Last access : 25 Juli 2011.

[3.] Munir, Rinaldi, 2006. "*Algoritma RSA dan Elgamal*", IF-ITB .

[4.] Sari, Deasy Ramadiyan, "*Keamanan SSL dalam Serangan Internet* ", Teknik Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.

[5.] Pratama, Satya Fajar. 2007. "*Algoritma Elgamal untuk Keamanan Aplikasi e-mail* ", Program Studi Teknik Informatika, Institut Teknologi Bandung.

[6.] *http://id.wikipedia.org/wiki/Surat_elektronik*
Last access : 2 Februari 2011.

[7] Wahyudiarto, Firmansyah, 2010, *http://ruwaifi.0fees.net/2010/10/macam-macam-enkripsi/,*
Last access : 3 Februari 2011.