Implementasi algoritma kriptografi kunci – publik ElGamal untuk keamanan pengiriman Email

M. Syaiful Rizal
7408040527
kambingjantan@student.eepis-its.edu

A. Abstrak

Kehidupan kita saat ini dilingkupi oleh *kriptografi*. Mulai dari transaksi di mesin ATM, percakapan melalui telpon genggam, mengakses Internet, sampai mengaktifkan peluru kendalipun menggunakan *kriptografi*. Begitu pentingnya *kriptografi* untuk keamanan Informasi (*Information Security*), sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan computer, maka tidak akan bisa dipisahkan dari dengan *kriptografi.*

Kriptografi juga digunakan dalam proses pengiriman *Email*. Jika sebuah *email* dikirim melewati jaringan *public* maka tingkat keamanannya sangat beresiko. Teknik – teknik pencurian informasi dari sebuah email ini semakin canggih dari hari ke hari. Salah satunya adalah konsep *Man – In – The Middle*. Penggunaan Kriptografi akan sangat membantu memberikan keamanan informasi email kita. Walaupun attacker atau *Man – In – the Middle* berhasil mendapatkan teks yang kita kirim namun tidak bisa mendapatkan informasi apapun karena teks yang didapat sudah ter-enkripsi sebelumnya. *Chipertek*s yang didapat hanya bisa dibuka oleh pihak yang memiliki *kunci private* (kunci untuk dekripsi).

Salah satu algoritma yang digunakan untuk *Enkripsi* dan dibahas dalam proyek akhir ini adalah algoritma *ElGamal*. Algoritma ini menekankan pada permasalahan *Algoritma diskrit*. Dengan permasalahan tersebut maka chiperteks hasil enkripsi *ElGamal* akan sangat sulit di *kriptanalis*.

Kata kunci : kriptografi, email, ElGamal, *Man in The Middle,* jaringan publik

Abstract

Our current life surrounded by cryptography. Starting from the transaction at the ATM machine, a conversation through mobile phones, accessing the Internet, to enable the missile was using cryptography. Once the importance of cryptography for Information Security (Information Security), so if talk about security issues associated with computer use, it will not be separated from the cryptography.

Cryptography is also used in the process of sending email. If an email is sent through the public network then the security level is very risky. Theft techniques of information from an email will increasingly from day to day. One of them is the concept of Man - In - The Middle. Use of Cryptography will help give our email information security. Although the attacker or the Man - In - The Middle managed to get the text that we send, but can not get any information obtained since the text had been encrypted before. Chipertext obtained can only be opened by the party who has a private key (decryption key).

One algorithm used for encryption and discussed in this final project is the ElGamal algorithm. This algorithm emphasizes the discrete algorithm problem. With these problems then chipertext ElGamal encryption result will be very difficult to decrypted.

Keyword : cryptography, email, ElGamal, Man in The Middle, public network

B. Latar Belakang

Kehidupan kita saat ini dilingkupi oleh *kriptografi*. Mulai dari transaksi di mesin ATM, percakapan melalui telpon genggam, mengakses Internet, sampai mengaktifkan peluru kendalipun menggunakan *kriptografi*. Begitu pentingnya *kriptografi* untuk keamanan Informasi (*Information Security*), sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan computer, maka tidak akan bisa dipisahkan dari dengan *kriptografi*[1].

Kriptografi juga digunakan dalam proses pengiriman *Email*. Jika sebuah *email* dikirim melewati jaringan *public* maka tingkat keamanannya sangat beresiko. Teknik – teknik pencurian informasi dari sebuah email ini semakin canggih dari hari ke hari. Salah satunya adalah konsep *Man – In – The Middle*. Penggunaan Kriptografi akan sangat membantu memberikan keamanan informasi email kita. Walaupun attacker atau *Man – In – the Middle* berhasil mendapatkan teks yang kita kirim namun tidak bisa mendapatkan informasi apapun karena teks yang didapat sudah ter-enkripsi sebelumnya. *Chipertek*s yang didapat hanya bisa dibuka oleh pihak yang memiliki *kunci private* (kunci untuk dekripsi).

Salah satu algoritma yang digunakan untuk *Enkripsi* dan dibahas dalam proyek akhir ini adalah algoritma *ElGamal*. Algoritma ini menekankan pada permasalahan *Algoritma diskrit*.[2] Dengan permasalahan tersebut maka chiperteks hasil enkripsi *ElGamal* akan sangat sulit di *kriptanalis*.

Matematika diskrit yang dimaksud dalam kriptografi El gamal adalah, mencari sebuah bilangan pangkat (x), pada sebuah bilangan bulat (g). Dimana bilangan tersebut *kongkruen* dengan bilangan bulat lainnya (y) jika di mod dengan bilangan p (bilangan prima) . kerumitannya terletak pada masalah diskrit karena melibatkan bilangan prima p sebagai variabel modulo dan x adalah bilangan yang dicari berupa bilangan pangkat.

Dengan proyek akhir ini diharapkan dapat membantu memberikan keamanan pada pengiriman email. Sehingga informasi yang penting butuh waktu lama dan sulit untuk dipecahkan, walapun fisik dari chipertext berhasil didapatkan oleh kriptanalis.

C. Tujuan

Penulis tertarik untuk menulis dan membahas tentang kriptografi ElGamal pada Email. Dengan tujuan menghasilkan sebuah aplikasi email client yang dapat :

- Mengirimkan pesan berupa chiperteks hasil enkripsi dari kunci publik tujuan (penerima) dengan kriptografi ElGamal.
- Menerima pesan dan membaca plainteks hasil dekripsi dari kunci private penerima pesan dengan kriptografi ElGamal.
- Membuat teks yang dikirimkan seolah – olah tidak memiliki informasi apapun, sehingga attacker (Man In The Middle) tidak bisa mendapatkan informasi dari email tersebut.

D. Permasalahan

Adapun permasalahan yang diangkat dalam proyek akhir ini adalah :

- Bagaimana membangkitkan bilangan acak (prima dan tidak prima) untuk menjadi kunci dalam sistem kriptografi ?
- Bagaimana mempublikasi kunci public dan menyembunyikan kunci private ?
- Bagaimana menghitung sebuah operasi perpangkatan yang menghasilkan sebuah bilangan bulat yang sangat besar sehingga tidak bisa ditampung oleh tipe data apapun dalam sebuah resource program (JAVA) ?
- Bagaimana menghitung operasi modulo dari sebuah bilangan bulat yang sangat besar tersebut ?
- Bagaimana menghitung operasi inversi modulo dari sebuah bilangan bulat yang sangat besar ?
- Bagaimana konversi karakter plainteks ke chiperteks atau sebaliknya dengan menggunakan tabel ASCII, dimana jumlah maksimal karakter ASCII harus bilangan prima ?
- Bagaimana membuat sebuah Email Client yang sudah disusupi oleh kriptografi ?
- Bagimana cara mengirim email teks dimana secara otomatis sudah dienkripsi dengan melihat kunci public tujuan email secara otomatis ?
- Bagaiman cara membuka sebuah email teks yang secara otomatis sudah di dekripsi ?
- Bagaimana membuat Email Client dengan menggunakan JAVA ?

E. Batasan Masalah

Pembatasan ruang lingkup (Batasan Masalah) penelitian adalah sebagai berikut :

- Enkripsi dan dekripsi pesan (Email) hanya data berupa teks (String atau tulisan)
- Algoritma yang dipakai adalah Algoritma ElGamal
- Bahasa pemrogman yang digunakan adalah JAVA.
- Menggunakan file Text untuk menyimpan data.
- Email Client hanya dapat mengirim dan membaca pesan.
- System operasi menggunakan Linux.

F. Teori Penunjang

a. Mail Client

Surat elektronik sudah mulai dipakai di tahun 1960-an. Pada saat itu Internet belum terbentuk, yang ada hanyalah kumpulan 'mainframe' yang terbentuk sebagai jaringan. Mulai tahun 1980-an, surat elektronik sudah bisa dinikmati oleh khalayak umum. Sekarang ini banyak perusahaan pos di berbagai negara menurun penghasilannya disebabkan masyarakat sudah tidak memakai jasa pos lagi [5].

Untuk mengirim surat elektronik kita memerlukan suatu program E*mail-client.* Dengan program inilah kita dapat mengirimkan email kita pada alamat tujuan melalui jarinan public, dengan menggunakan protokol SMTP. Sedangkan untuk dapat menerima pesan, hasil kiriman pihak lain untuk kita, maka Email Client menggunakan protocol POP3 atau IMAP.

Keamanan data di surat elektronik tidaklah terjamin dan selalu ada risiko terbuka untuk umum, dalam artian semua isinya dapat dibaca oleh orang lain. Hal ini disebabkan oleh karena surat elektronik itu akan melewati banyak *server* sebelum sampai di tujuan. Tidak tertutup kemungkinan ada orang yang menyadap surat elektronik yang dikirimkan tersebut. [5].

Surat elektronik dapat diamankan dengan melakukan teknik pengacakan (enkripsi). Salah satu program enkripsi yang populer adalah PGP (*Pretty Good Privacy*). Dengan memakai PGP maka isi akan dienkrip, dan hanya orang yang tertuju dapat mendekripsi dan membaca surat elektronik tersebut.

Kerugiannya adalah membuat repot pihak pengirim dan penerima (karena keduanya harus memiliki program PGP, dan pengirim juga harus memiliki kunci umum penerima, dan melakukan enkripsi pesan dengan kunci tersebut). [5].

b. Kriptografi ElGamal

Algoritma ElGamal dibuat oleh Taher ElGamal pada tahun 1984. Algoritma ini pada mulanya digunakan untuk tanda tangan digital atau *digital signature.* Namun kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan dekripsi. ElGaMal digunakan dalam perangkat lunak yang dikembangkan oleh GNU, program PGP, dan pada program keamanan jaringan lainnya. Keamanan algoritma ini terletak pada sulitnya menghitung algoritma diskrit.

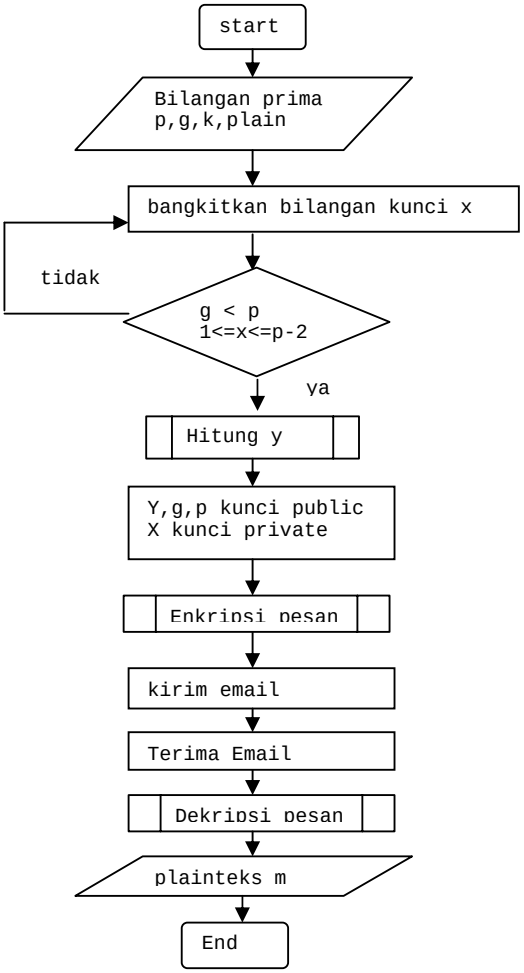
Masalah algoritma diskrit adalah, jika p adalah bilangan prima dan g dan y adalah sembarang bilangan bulat. Carilah x sedemikian sehingga $g^x \equiv y \pmod p$.

Besaran - besaran yang digunakann dalam algoritma ElGamal adalah[6] :

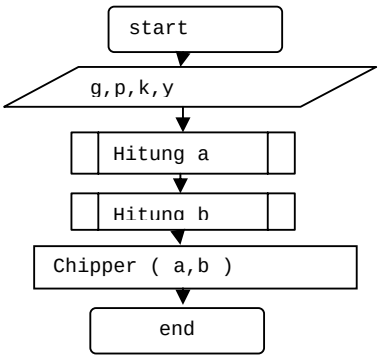
1) Bilangan Prima p (Publik)
2) Bilangan acak, g (g<p) (Publik)
3) Bilangan acak,x (x<p-3) (Privat)
4) $y = g^x \bmod p$ (Publik)
5) m (Plainteks) (Privat)
6) a dan b (Chiperteks) (Publik)

G. Perancangan Sytem

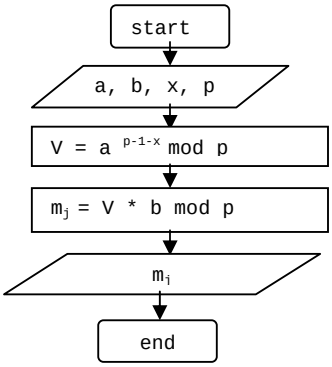
Mail client pengirim pesan melakukan enkripsi dengan mengirim parameter plain text terhadap fungsi enkripsi. Setelah itu fungsi enkripsi mengirimkan chipertext sebagai hasil dari enkripsi. Dengan port dan protokol SMTP maka pesan berupa chipertext dikirim ke mail server. Mail server mengirim ke mail server tujuan jika si penerima memiliki mail server berbeda. Dengan protokol POP3 atau Imap maka mail client penerima pesan dapat menerima email tersebut. Penerima Email dapat melakukan dekripsi dengan mengirimkan parameter chipertext. Fungsi dekripsi akan melakukan pengecekan kunci privat terlebih dahulu. Setelah kunci privat di masukkan maka fungsi dekripsi dapat mengirim plain text hasil dekripsi. Inti dari program diatas adalah Mail Client dapat mengirim email ke mail server setelah melakukan enkripsi. Dan mail client penerima dapat mendownload kiriman email di Mail Server, lalu melakukan dekripsi. Berikut adalah beberapa flowchart dalam sistem proyek akhir ini.



Gambar 1. Flowchart Umum



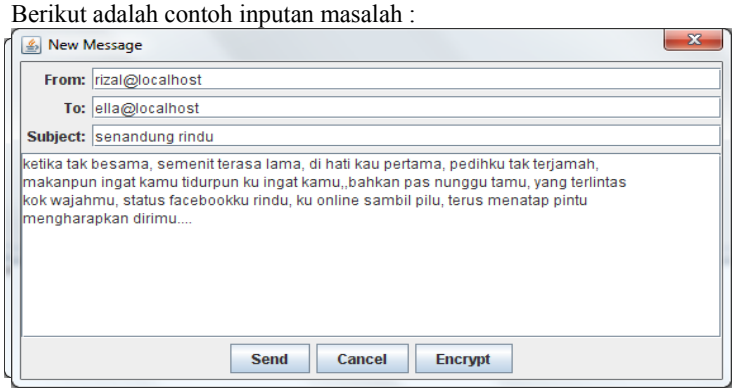
Gambar 2. Flowchart Enkripsi



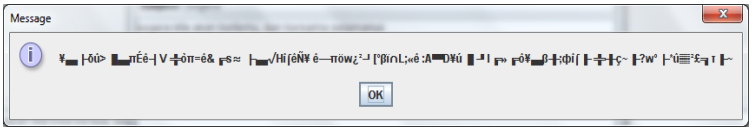
Gambar 3. Flowchart Dekripsi

H. Ujicoba dan Analisa

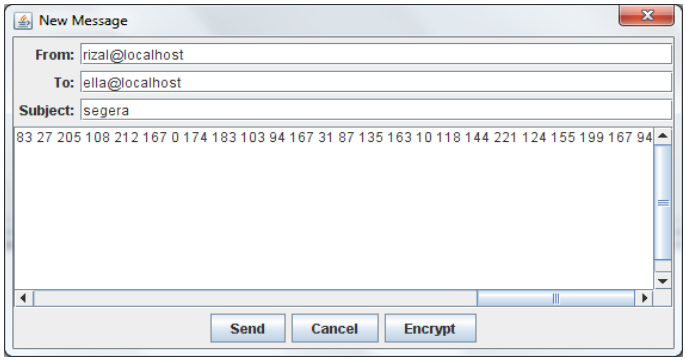
Berikut adalah contoh inputan masalah :



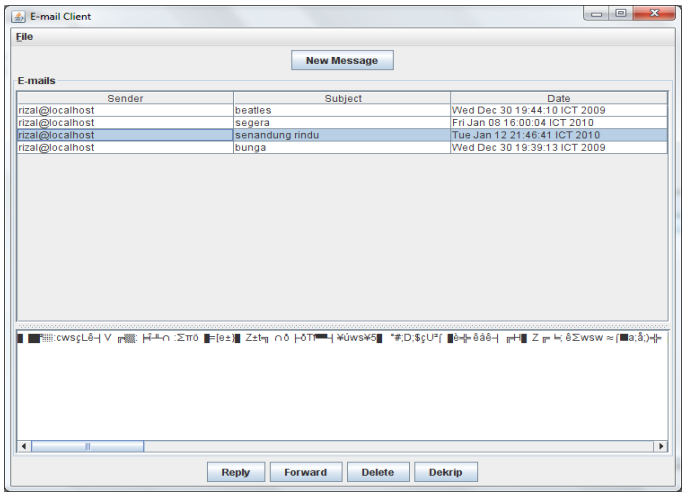
Gambar 4. Contoh email yang akan dikirm



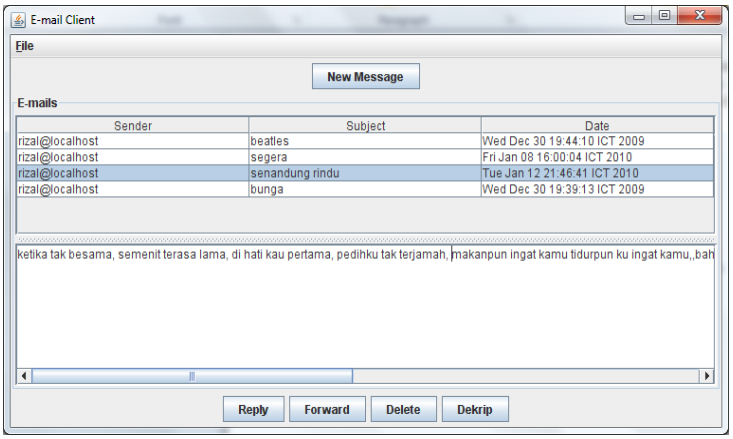
Gambar 5. Contoh hasil enkripsi



Gambar 6. Contoh email setelah enkripsi



Gambar 7. Contoh Inbox sebelum di enkripsi



Gambar 8. Contoh Inbox setelah di enkripsi

I. Penutup

a. Kesimpulan

Berdasarkan hasil percobaan dan analisa yang dilakukan pada Proyek Akhir ini maka dapat disimpulkan bahwa :

1) Sistem yang dibuat sudah mampu memenuhi kebutuhan sebagai aplikasi Mail Client yang menerapkan kriptografi ElGamal.
2) Semua karakter dapat di enkripsi dengan sempurna berdasar *public key*, kecuali karakter ”\n” atau ”Enter” yang dikenali sebagai spasi.
3) Proses pengiriman Email (berupa *chipertext*) dilakukan dengan mengirimkan bilangan ASCII dari karakter *chipertext-nya.*
4) Proses dekripsi berjalan dengan sempurna.
5) Proses *enkripsi* memperlambat pengiriman email. Namun tidak mengganngu, karena email tidak mebutuhkan waktu yang *real time* seperti *chatting.*
6) Daftar karakter *unicode* yang digunakan sebanyak 223 karakter saja.

b. Saran

Berikut merupakan beberapa saran untuk pengembangan sistem di masa yang akan datang, berdasar pada hasil perancangan, implementasi, dan uji coba yang telah dilakukan. :

1) Menambah karakter Unicode sehingga range kunci x juga bertambah besar, dan menambah keamanan kriptografi ElGamal.
2) Menyempurnakan algoritma Enkripsi dalam kasus mengenali “\n” sebagai spasi.
3) Pembuatan antarmuka aplikasi berupa WAP atau aplikasi Web Service, sehingga aplikasi ini bisa diakses dari berbagai macam platform.

J. Daftar Pusatka

1. Rinaldi, Munir ” *Kriptografi* ” Penerbit Informatika oktober 2006
2. Ariyus, Dony ”*Pengantar Ilmu Kriptografi*” Penerbit Andi 2008
3. *www.AsciiTable.com, ”ASCII Table, 2009*
4. http://agcrypt.wordpress.com/ ”kriptografi-apa-sih ?”,2008
5. www.Wikipedia.com/email client ,”Email Client”, 2006
6. www.embek-poenya-selera.com, ”Kriptografi Moderen”,2008