KRIPTOGRAFI ELGAMAL MENGGUNAKAN METODE MERSENNE

Triase, ST, M. Kom

ABSTRAK

Untuk mengamankan sebuah data dalam komputerisasi diperlukan teknik kriptografi. Salah satu teknik kriptografi penyandian adalah menggunakan Algoritma Elgamal. Algoritma Elgamal merupakan bagian dari kriptografi asimetris yang pembentukan salah satu kuncinya menggunakan bilangan prima dan menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit. Dengan memanfaatkan bilangan prima yang besar serta masalah logaritma diskrit yang cukup menyulitkan, maka keamanan kuncinya lebih terjamin. Adapun algoritma untuk pembangkitan bilangan prima tersebut adalah menggunakan metode Mersenne. Proses enkripsi ElGamal dari plaintext ke dalam bentuk ciphertext didahului pembentukan kunci oleh penerima pesan, dua macam pasangan kunci yaitu kunci public dan kunci private. Kunci public untuk disebar luaskan sedangkan kunci private untuk diri sendiri. Untuk membuat sebuah pesan rahasia dalam bentuk ciphertext, pesan rahasia harus dikonversikan terlebih dahulu dalam bilangan bulat kemudian dikodekan berdasarkan kode ASCII(*American Standart for Information Interchange*). Pesan dalam bentuk ciphertext didekripsi menggunakan kunci private untuk dikembalikan menjadi pesan yang sebenarnya. Sehingga Kriptografi Elgamal melindungi pesan rahasia dengan aman.

Kata Kunci : Algoritma ElGamal, Kriptografi asimetris, Mersenne, enkripsi, dekripsi, pesan rahasia, ciphertext, plaintext, kunci publik, kunci private.

LATAR BELAKANG MASALAH

Perkembangan yang pesat di bidang telekomunikasi dan komputer dewasa ini telah berpengaruh pada hampir semua aspek kehidupan manusia, salah satunya dalam hal berkomunikasi. Dengan adanya internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan murah. Namun disisi lain, ternyata internet tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan oleh siapapun sehingga sangat rawan terhadap penyadapan atau serangan informasi oleh pihak-pihak yang tidak berhak (*unauthorized person*) untuk mengetahui informasi tersebut. Oleh karena pengguna internet yang sangat luas seperti pada perdagangan, bisnis, bank, industri dan pemerintahan yang umumnya mengandung informasi yang bersifat rahasia maka keamanan informasi menjadi faktor utama yang harus dipenuhi. Berbagai hal yang telah

dilakukan untuk mendapatkan jaminan keamanan informasi rahasia ini. Salah satu cara yang digunakan adalah dengan menyandikan isi informasi menjadi suatu kode-kode yang tidak dimengerti sehingga apabila disadap maka akan kesulitan untuk mengetahui isi informasi yang sebenarnya.

Masalah keamanan merupakan suatu aspek penting dalam pengiriman data maupun informasi melalui jaringan. Hal ini disebabkan karena kemajuan di bidang jaringan komputer dengan konsep *open system*-nya sehingga memudahkan seseorang untuk masuk ke dalam jaringan tersebut. Hal tersebut dapat mengakibatkan proses pengiriman data menjadi tidak aman

Kriptografi merupakan metode untuk mengamankan data, baik data teks maupun data gambar. Metode ini dilakukan dengan penyandian atau pengacakan data asli, sehingga pihak lain yang tidak mempunyai hak akses atas data tersebut tidak memperoleh informasi yang ada di dalamnya. Ilmu kriptografi sebenarnya telah lama digunakan, sejak jaman sebelum mengenal metode pengiriman data menggunakan komputer. Metode penyandian pertama kali dibuat masih menggunakan metode algoritma rahasia. Metode ini menumpukan keamanannya pada kerahasian algoritma yang digunakan. Namun metode ini tidak efisien saat digunakan untuk berkomunikasi dengan banyak orang. Oleh karena itu seseorang membuat algoritma baru apabila akan bertukar informasi rahasia dengan orang lain.

Karena penggunaanya yang tidak efisien maka algoritma rahasia mulai ditinggalkan dan diperkenalkan suatu metode baru yang disebut dengan algoritma kunci. Metode ini tidak menumpukan keamanan pada algoritmanya, tetapi pada kerahasiaan kunci yang digunakan pada proses penyandian. Algoritmanya dapat diketahui, digunakan dan dipelajari oleh siapapun. Metode algoritma kunci mempunyai tingkat efisiensi dan keamanan yang lebih baik dibandingkan dengan algoritma rahasia. Sampai sekarang algoritma kunci masih digunakan secara luas di internet dan terus dikembangkan untuk mendapatkan keamanan yang lebih baik. Hukum Kerchkoff menyatakan " Algoritma tidak perlu dirahasiakan, tetapi kuncinya harus rahasia".

Berdasarkan jenis kunci, algoritma kriptografi dibagi menjadi dua yaitu kunci simetris dan kunci asimetris. Algoritma kriptografi yang menggunakan kunci simetris, yakni DES, 3DES, IDEA, AES, *Blowfish*, *Twofish* dan lain-lain. Sedangkan Algoritma kriptografi yang menggunakan kunci asimetris, yakni RSA, MD5, *Elgamal* dan lain-lain.

Kriptografi Elgamal dalam pembentukan salah satu kuncinya menggunakan bilangan prima dan menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit. Sehingga dengan memanfaatkan bilangan prima yang besar dan serta masalah logaritma diskrit yang cukup menyulitkan, maka keamanan kuncinya akan

lebih terjamin(Siti Nur Hamidah, 200).

Pembangkitan bilangan prima adalah sebuah permasalahan yang esensial di dalam ilmu komputer dan teori bilangan, terutama dalam bidang kriptografi. Hal ini dikarenakan protokol-protokol enkripsi kunci publik didasarkan pada penggunaan dari bilangan prima dengan ukuran besar. Sedangkan keamanan sistem kriptografi kunci publik sering didasarkan pada kesulitan untuk mendapatkan faktor-faktor prima dari suatu bilangan prima yang sangat besar.

Dalam dunia komputer sudah ditemukan beberapa cara untuk mencari bilangan prima tersebut, oleh karena itu penulis mencoba untuk menggunakan metode *Mersenne* untuk mencari bilangan prima tersebut.

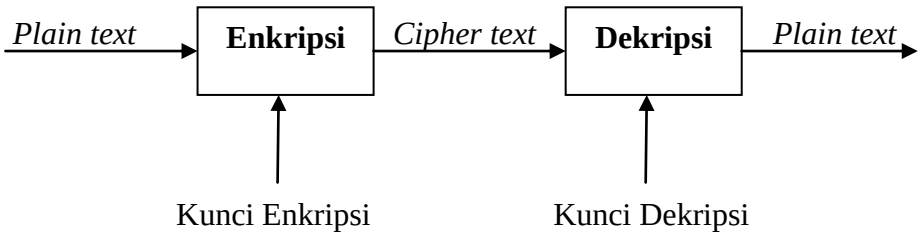
LANDASAN TEORI

Menurut Richard Mollin (2003), Kriptografi (cryptography) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes, Oorscoot dan Vanstone, 1996). Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptorafi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan.

Berdasarkan beberapa definisi kriptografi di atas, dapat disimpulkan bahwa Kriptografi merupakan ilmu sekaligus seni untuk menjaga kerahasiaan data atau informasi agar tidak dapat di lihat, dibaca, dimengerti oleh pihak ketiga yang tidak memiliki wewenang terhadap data atau informasi tersebut.

Kriptonalisis (*cryptanalysis*) adalah kebalikan dari kriptografi, yaitu suatu ilmu untuk memecahkan mekanisme kriptografi dengan cara mendapatkan kunci dari *ciphertext* yang digunakan untuk mendapatkan *plaintext*. Kriptologi *(cryptology)* adalah ilmu yang mencakup kriptografi dan kriptonalisis.

Kriptografi terdiri dari dua proses utama yaitu proses enkripsi dan dekripsi. Adapun diagram proses enkripsi dan dekripsi secara umum, dapat di lihat pada gambar 2.1. (Candra, 2005).



Gambar 2.1. Diagram Proses Enkripsi dan Dekripsi Secara Umum

Berdasarkan gambar 2.1., maka dapat dibuat notasi matematika dalam proses enkripsi dan dekripsi yaitu :

$$E_e(P) = C \quad .....(1)$$
$$D_d(C) = P \quad .....(2)$$

Keterangan :
(1) = Persamaan proses enkripsi
(2) = Persamaan proses dekripsi
E = Enkripsi
D = Dekripsi
C = Cipher text
P = Plain text
e = Kunci Enkripsi
d =Kunci Dekripsi

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi yaitu:

a. *Kerahasiaan,* adalah aspek yang berhubungan dengan penjagaan isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah dienkripsi.
b. *Integritas data,* adalah aspek yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
c. *Autentikasi,* adalah aspek yang berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang kirimkan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
d. *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerimaan pesan menyangkal telah menerima pesan. Sebagai contoh, misalnya pengiriman pesan memberi otoritas kepada penerima pesan untuk melakukan pembelian namun kemudian ia meyangkal telah memberikan otoritas tersebut (Rinaldi munir, 2004)

Kriptografi ElGamal pertama kali dipublikasikan oleh Taher ElGamal pada tahun 1985.

Kriptografi ElGamal pada mulanya digunakan untuk digital signature, namun kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan deskripsi. Kriptografi ElGamal digunakan kedalam perangkat lunak sekuriti yang dikembangkan oleh GNU, program PGP, dan pada sistem sekuriti lainnya. Kriptografi ElGamal tidak dipatenkan oleh pembuatnya melainkan didasarkan atau penyempurnaan dari pada kriptografi Diffei-Hellman, yaitu sebuah kriptografi kunci publik yang dikenalkan oleh Whitfield Diffie dan Martin Hellman. Sehingga hak paten kriptografi Diffie-Hellman mencakup kriptografi ElGamal. Dan hak paten ini telah berakhir pada tahun 1997 sehingga mulai saat itu kriptografi ElGamal dapat di komersilkan secara umum (Mulyana, 2009).

Kriptografi Elgamal merupakan bagian dari kriptografi asimetris. Kunci asimetris biasa dikenal dengan nama *public key*(kunci public) dan *private key*(kunci pribadi). Kunci asimetris adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci publik dan kunci privat. Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan. Pada umumnya kunci publik digunakan sebagai kunci enkripsi sementara kunci privat digunakan sebagai kunci dekripsi.

Logaritma Diskrit

Kriptograf Elgamal menggunakan konsep logaritma diskrit(Budi Murtiyasa, 2004). Menurut Shao (1998) telah mengembangkan konsep autentikasi kunci publik berdasarkan faktorisasi dan logaritma diskrit. Sebelum membahas tentang sistem kriptografi ElGamal, akan dijelaskan tentang masalah logaritma diskret.

Misalkan G adalah suatu grup siklik dengan order *n,α* adalah pembangun G dan elemen identitas dari G adalah 1. Diberikan γ Є G Masalah yang dimunculkan ialah bagaimana menentukan suatu bilangan bulat nonnegatif terkecil *b* sedemikian sehingga memenuhi :

$$\gamma \equiv \alpha^b \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Bilangan bulat *b* seperti ini disebut dengan logaritma diskret dari γ dengan basis α. Masalah bagaimana untuk menentukan bilangan bulat *b* seperti ini disebut dengan masalah logaritma diskret. Masalah komputasi logaritma diskret sangat penting dalam kriptografi. Banyak kegiatan kriptografi yang tumpuan keamanannya menggunakan masalah logaritma diskret. Misalnya digunakan sebagai dasar pembangkitan kunci pada sistem kriptografi ElGamal

Masalah logaritma diskrit adalah jika *p* adalah bilangan prima dan *g* dan *y* adalah sebarang bilangan bulat, carilah *x* sedemikian sehingga

$$y = g^x \bmod p \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$

Pembangkitan kunci

Langkah langkah dalam pembangkitan kunci

1. Pilih sembarang bilangan prima $p > 255$
2. Pilih dua buah bilangan acak, g dan x dengan syarat $g < p$ dan $1 \leq x \leq p-2$
3. Hitung $y=g^x \mod p$.
   y adalah bagian dari kunci publik, sehingga kunci publik algoritma ElGamal berupa pasangan 3 bilangan, yaitu (y,g,p).Sedangkan kunci rahasianya adalah bilangan x tersebut.

a. Metode Enkripsi

Pada proses ini pesan dienkripsi menggunakan kunci publik (y,g,p) dan sembarang bilangan acak rahasia k anggota (0,1,…,p-2). Misalkan m adalah pesan yang akan dikirim. Selanjutnya, m diubah ke dalam blok-blok karakter dan setiap karakter dikonversikan ke dalam kode ASCII, sehingga diperoleh plainteks $m_1,m_2,\ldots,m_n$ dengan m_i anggota {1,2,…,p-1}, i=1,2,…,n.

Langkah-langkah dalam mengenkripsi pesan:

1. Susun Plainteks menjadi blok-blok $m_1,m_{2,},\ldots,m_n$ dengan setiap blok adalah suatu karakter pesan
2. Konversikan masing-masing karakter ke dalam kode ASCII, maka diperoleh plainteks sebanyak n bilangan, yaitu $m_1,m_{2,},\ldots,m_n$
3. Untuk i dari 1 sampai n kerjakan:
   a. Pilih sebarang bilangan acak rahasia ki ε {0,1,…,p-2}
   b. Hitung $a_i = g^{ki} \mod p$……(5)
   c. $b_i = y^{ki}m_i \mod p$……(6)
4. Diperoleh *ciphertext* yaitu $(a_{i,},b_i)$
   Diperoleh *ciphertext* yaitu $(a_{i,},b_i),i$ = 1,2,…n.Jadi ukuran *ciphertext* dua kali ukuran *plainteksnya*.

b. Metode Dekripsi

Setelah menerima *ciphertext* (a,b), proses selanjutnya adalah mendekripsi *cipherteks* menggunakan kunci publik p dan kunci rahasia x. Dapat ditunjukkan bahwa *plaintext* m dapat diperoleh dari *ciphertext* menggunakan kunci rahasia x.

Langkah-langkah dalam mendekripsi pesan:

1. *Ciphertext* $(a_{i,},b_i)$, i = 1,2,…,n, kunci publik p dan kunci rahasia x.
2. Untuk i dari 1sampai n kerjakan:
   a. Hitung $a_i^{p-1-x} \mod p$……..(7)
   b. Hitung $m_i=bi/ai^x \mod p = bi(ai^x)^{-1} \mod p$……(8)
3. Diperoleh *plaintext* $m_1,m_{2,},\ldots,m_n$

   Konversikanmasing-masimg $m_1,m_{2,},\ldots,m_n$ ke dalam karakter sesuai dengan kode ASCII-nya, kemudian hasilnya digabungkan kembali.

Prima Mersenne

Bilangan prima mersenne adalah jenis khusus bilangan prima. Bilangan Prima Mersenne

ditemukan setelah bilangan prima Fermat, ditemukan seolah menyempurnakannya. Seorang ilmuwan Prancis, Marin Mersenne, membuat suatu bentuk baru dari bilangan prima yang akhirnya namanya diabadikan menjadi nama bilangan ini yaitu bilangan prima Mersenne (Mersenne prime). Rumus untuk menghitung bilangan prima ini kelihatannya sederhana tetapi pada pehitungannya sangat kompleks.

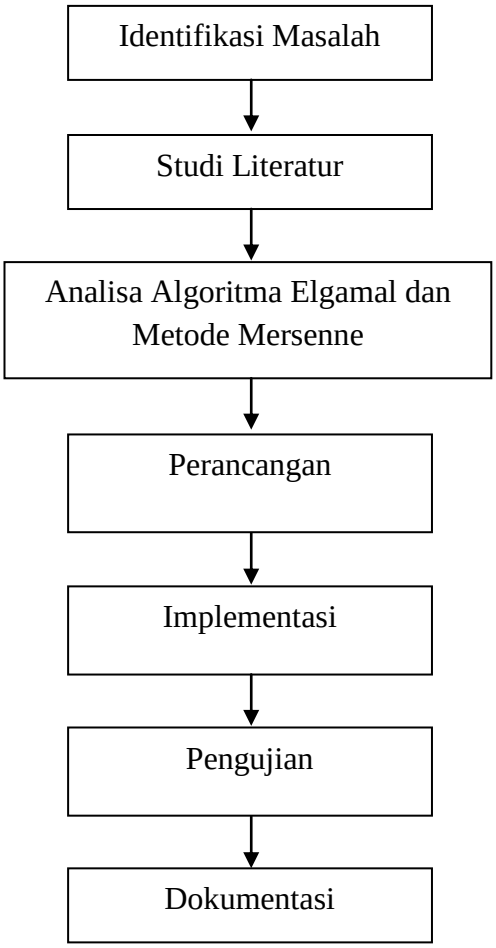
Bilangan prima Mersenne adalah bilangan bulat dari rumus: $M_p = 2^p - 1$…….(9)

dimana $p \geq 3$

Dengan p adalah bilangan prima(Sibao Zhang, dkk, 2010).

METODOLOGI

Metodologi ini merupakan tahapan-tahapan yang akan dilakukan dalam menyelesaikan masalah yang akan dibahas agar penelitian dapat berjalan dengan baik, mulai dari identifikasi masalah, studi literatur, analisa algoritma Elgamal dan metode mersenne, perancangan pembentukan kunci dan prosedur kripto, implementasi, pengujian, hingga dokumentasi.



Gambar 3.1. Kerangka Kerja

Berdasarkan kerangka kerja pada gambar 3.1. maka masing-masing langkah dapat diuraikan sebagai berikut :

1. Identifikasi Masalah
   Pada tahapan ini masalah yang diidentifikasi adalah mengamankan pesan rahasia dalam bentuk file dokumen berupa file *.txt agar file tersebut dapat diterima oleh penerima dengan aman.
2. Studi Literatur
   Studi literatur dilakukan untuk mempelajari dan melengkapi pengetahuan yang berkaitan dengan metode kriptografi Elgamal dan Mersenne yang dimiliki peneliti, Sumber literatur berupa buku, jurnal, paper, karya ilmiah maupun situs-situs internet penunjang lainnya
3. Analisa Algoritma Elgamal dan Metode Mersenne
   Pada tahapan ini, dianalisa lebih mendalam tentang pembentukan algoritma Elgamal dan metode mersenne. Langkah pertama yang dilakukan adalah menguji algoritma yang ada dengan data coba secara manual, sebelum diimplementasikan ke dalam program. Diantaranya pembentukan kunci, enkripsi dan dekripsi. Kemudian menganalisa bagaimana memanfaatkan Algoritma Elgamal dengan menggunakan bilangan prima yang didapatkan dari metode mersenne sehingga dapat merancang program enkripsi dan dekripsi.
4. Perancangan
   Pada tahapan ini untuk mempermudah dalam pengimplementasian system maka dilakukan perancangan system aplikasi menggunakan flow chart. Alur Perancangan di mulai dari perancangan tampilan program, perancangan kunci kriptografi, perancangan prosedur enkripsi dan dekripsi yang akan dibuat penulis. Tampilan program bersifat *user-friendly* atau mudah digunakan oleh pengguna.
5. Implementasi
   Pada tahapan ini dilakukan untuk mengimplementasikan hasil rancangan dan analisis di atas. Kemudian dilakukan pembuatan program, pembuatan antarmuka masukan dan keluaran, dan antarmuka proses enkripsi dan dekripsi pada algoritma Elgamal menggunakan metode mersenne. Dalam proses pembuatan program enkripsi dan dekripsi dengan menggunakan algoritma Elgamal dan metode mersenne , penulis menggunakan spesifikasi sebagai berikut :
   1) Perangkat Keras
      a. Processor Intel N280
      b. Memory 1 GB
      c. Hardisk 116 GB
      d. Mouse, Keyboard, Monitor, dan lain-lain
   2) Perangkat Lunak
      a. Sistem Operasi Microsoft Windows XP Professional SP2
      b. Aplikasi Java NetBeans IDE 7.0.
6. Pengujian
   Pada tahapan ini dilakukan mekanisme pengujian dengan cara menginputkan file dokumen berupa file *.txt yang akan dienkripsi. Kemudian system akan meminta input bilangan prima yang bertujuan untuk mendapatkan kunci publik dan kunci privat. Kunci privat berguna untuk mendekripsi file yang dienkrip tersebut. Sehingga apabila algoritma berjalan dengan benar maka akan dikembalikan file yang terenkripsi

tersebut akan menjadi file *.txt kembali.

7. Dokumentasi
   Tahapan ini penulis akan melaporkan hasil penelitian yang sudah dilakukan. Dokumen berisi laporan mulai dari identifikasi masalah hingga implementasi dan pengujian.

ANALISA DAN PERANCANGAN

Pada algoritma ElGamal ini terdiri dari tiga proses, yaitu proses pembangkitan pasangan kunci , proses enkripsi, dan proses dekripsi. Algoritma ini melakukan proses enkripsi pada blok-blok *plaintext* dan kemudian menghasilkan blok-blok *ciphertext* yang kemudian dilanjutkan dengan proses dekripsi, dimana hasilnya digabungkan kembali,sehingga menjadi pesan yang utuh dan mudah dipahami. Untuk pembentukan sistem kriptografi ElGamal, dibutuhkan bilangan prima *p*.

1. Proses Pengujian prima mersenne dengan Lucas Lehmer

Proses pengujian prima mersenne menggunkan metode lucas-Lehmer merupakan metode yang digunakan untuk membuktikan bilangan prima tersebut prima atau tidak. Apabila pada pengujian ditemukan bahwa Mp =0 maka bilangan tersebut adalah bilngan prima dan apabila Mp ≠ 0 maka bilangan tersebut bukan bilangan prima. Pada perhitungan bilangan prima mersenne diperlukan persamaan(9). Kemudian bilangan prima mersenne tersebut akan diuji keprimaannya menggunkan pengujian Lucas Lehmer. Dimana di dalam pengujian Lucas Lehmer metode yang digunakan menggunakan jenis pengujian kuadrat cepat. Untuk menyelesaikan pengujian Lucas Lehmer menggunakan persamaan(10).

Contoh 4.1

Bilangan prima yang akan di gunakan adalah bilangan prima 7. Apabila digunakan persamaan (9) yaitu $2^7 - 1$ adalah bilangan prima. Untuk membutikan keprimaan 7 menggunakan persamaan (10). Pembuktian :

$S_0 = 4$

$S_1 = (4 * 4 - 2) \bmod 127 = 14$

$S_1 = (14 * 14 - 2) \bmod 127 = 67$

$S_1 = (67 * 67 - 2) \bmod 127 = 42$

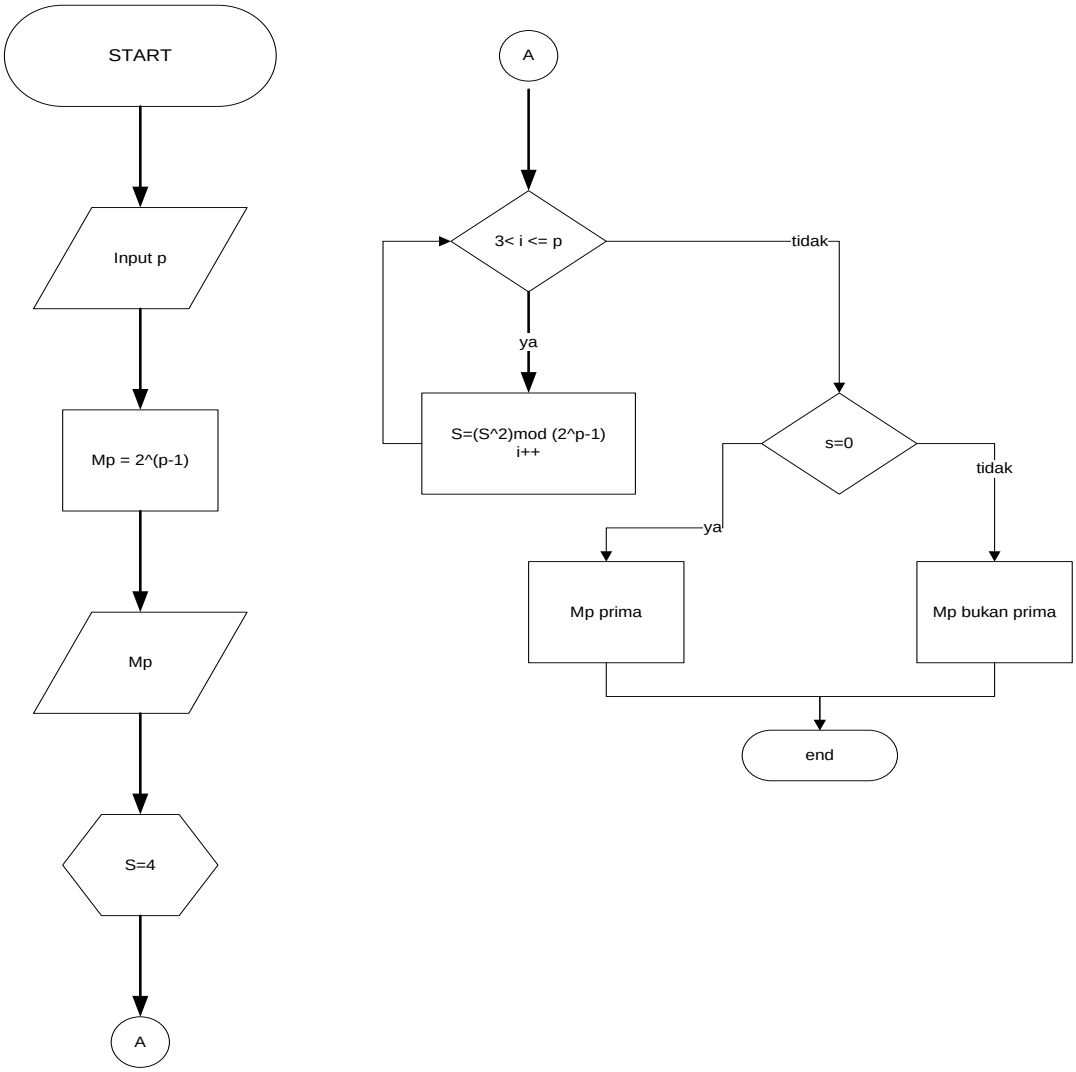
$S_1 = (42 * 42 - 2) \bmod 127 = 111$

$S_1 = (111 * 111 - 2) \bmod 127 = 0$

Terbukti bahwa $S_{p-2} = 0$, maka $2^7 - 1$ merupakan bilangan prima.

2. Flowchart Pengujian Prima Mersenne

Berikut ini prosedur kerja pengujian metode mersenne dengan Lucas Lehmer, yaitu dapat dilihat pada gambar *flowchart* berikut ini:



Gambar 4.1 Diagram Alir Pengujian Mersenne(Lucas-Lehmer)

3. Pemodelan Fungsional sistem

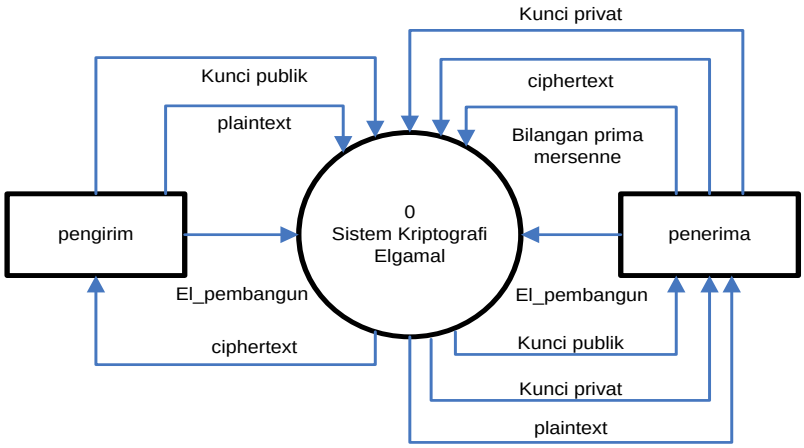
Hasil yang diharapkan dari tahapan membangun suatu sistem adalah bagaimana cara agar sistem yang dibangun memiliki kemampuan maksimal. Pada sistem kriptografi Elgamal memiliki tiga fungsi yaitu fungsi pembentukan kunci, fungsi enkripsi pesan dan fungsi dekripsi pesan. Dari ketiga fungsi tersebut terdapat fungsi – fungsi pendukung tersebut, seperti fungsi tes keprimaan untuk memeriksa bilangan prima yang digunakan apakah prima atau tidak, fungsi membangun kunci secara acak.

a. DFD Proses

Pemodelan fungsional digambarkan dengan diagram aliran data (DFD). DFD merupakan suatu pemodelan untuk menunjukkan bagaimana data mengalir dalam serangkaian proses di dalam sistem. DFD merupakan model dari sistem untuk menggambarkan pembagian sistem ke modul yang lebih kecil. Keuntungan menggunakan Data

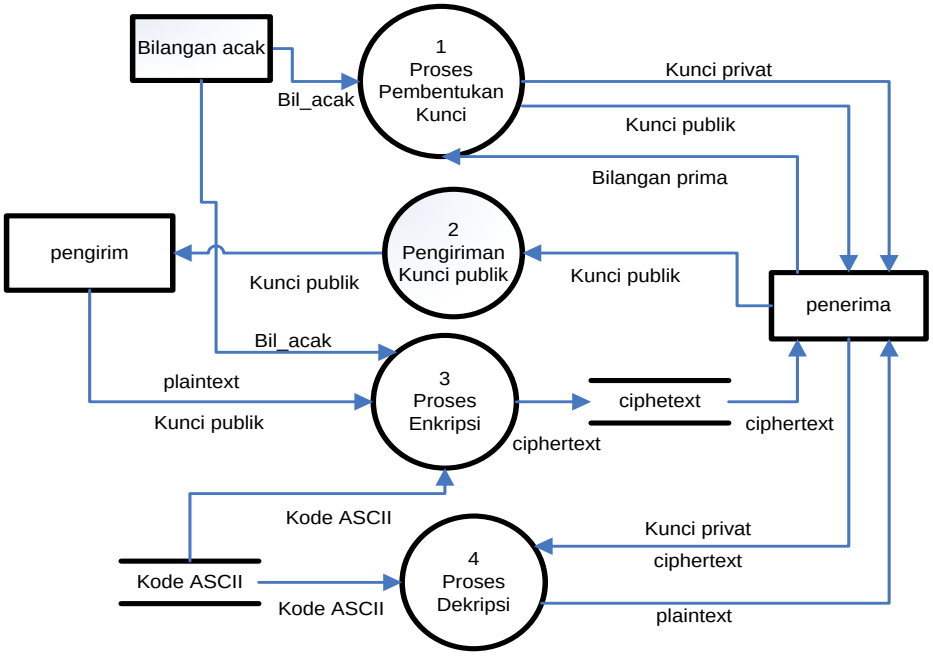
Flow Diagram memudahan pemakai untuk mengerti sistem yang akan dikerjakan atau dikembangkan. Simbol DFD yang akan digunakan dalam pembahasan ini adalah simbol De Marco atau Yourdan.

Data Flow Diagram dari perangkat Kriptografi Elgamal menggunakan metode mersenne yang penulis rancang. Diagram konteks tersebut dapat dilihat pada gambar 4.1, diagram level 1 dilihat pada gambar 4.2, dan diagram level 2 ditunjukan pada gambar 4.3, serta gambar 4.4 dan 4.5.



Gambar 4.1 Diagram Konteks

Pengembangan proses pada diagram Konteks dapat dijabarkan pada DFD level 0 berikut :



Gambar 4.2 DFD Level 0

Pada gambar DFD diagram level 0 di atas dapat dilihat terdapat 4 proses yang dapat dilakukan pada kriptosistem ini yaitu :

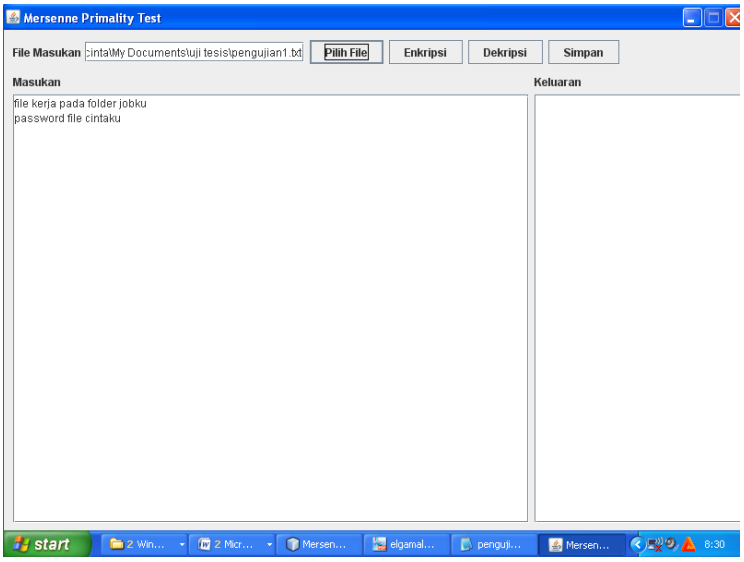
1. Proses Pembentukan Kunci
   Penerima melakukan proses pembentukan kunci untuk mendapatkan kunci publik, kunci privat yang didapatkan dari penginputan bilangan prima dan bilangan acak algoritma yang diinputkan oleh penerima ke dalam kripto sistem ini.
2. Proses pengiriman kunci
   Penerima mengirimkan kunci public kepada pengirim agar kunci public dapat digunakan untuk melakukan proses enkripsi
3. Proses Enkripsi
   Proses enkripsi yang dilakukan pengirim untuk mengubah file teks asli menjadi pesan terenkripsi yang tidak dapat dipahami berupa ciphertext. Adapun caranya adalah dengan melakukan konversi plaintext ke dalam kode ASCII kemudian dengan menggunakan kunci publik yang diperoleh dari penerima.
4. Proses Dekripsi
   Proses dekripsi merupakan proses yang dilakukan penerima untuk mengubah pesan yang telah dienkripsi menjadi pesan asli seperti semula. Untuk melakukan proses dekripsi ini penerima menggunakan ciphertext dan kunci privat serta kode ASCII.

Implementasi dan Pengujian Sistem

Pelaksanaa pengujian pada sistem kriptografi Elgamal menggunakan metode mersenne dilakukan setelah tahapan skenario pengujian dilakukan sebelumnya. File – file yang digunakan sama dengan file yang digunakan pada tahapan skenario. Adapun tahapan pelaksanaan pengujian enkripsi dan dekripsi file teks adalah sebagai berikut :

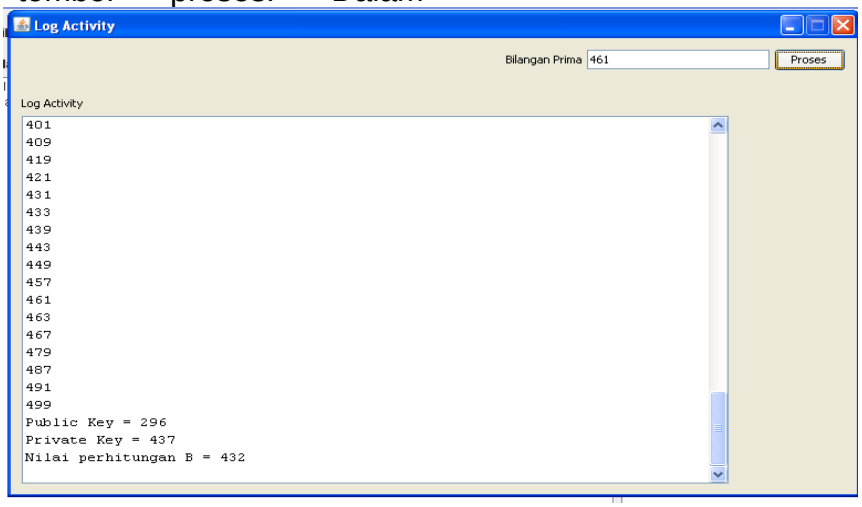
1. Proses key generation
   Pada tahap ini
2. Proses Enkripsi
   Pada tahap ini pertama sekali yang dilakukan adalah menyediakan file yang akan dienkripsi. File yang dienkiripsi berextention *.text. Ada beberapa file yang akan diuji. Nama filenya yaitu :
   - pengujian1.txt (file berisi karakter huruf)
   - pengujian2.txt (file berisi karakter angka)
   - pengujian3.txt (file berisi gabungan huruf, angka dan simbol)

   a. Mengklik menu pilih file untuk mengambil file yang tersimpan dalam drive. Untuk uji coba file yang penulis sediakan sebanyak 3 file, sehingga penulis melakukan pengujian terhadap file tersebut bergantian. Antar muka pemilihan file pengujian yang akan di enkrip terdapat pada gambar 5.7 berikut :



Gambar 5.7 Menu Pilih file pengujian1

b. Mengklik menu tombol enkripsi untuk mengenkrip file text pada sistem kriptografi Elgamal. Adapun yang diperlukan dalam enkripsi ini kunci publik yang dibentuk menggunakan bilangan prima mersenne. Cara membentuk kunci dengan menginputkan bilangan prima pada menu log activity kemudia tekan tombol proses. Dalam pengujian ini yang diuji adalah penggunaan bilangan prima yang sama untuk menguji file yang berbeda. Bilangan prima tersebut adalah "461". Gambar antar muka menu enkripsi sekaligus pembangkitan kunci publik dan kunci privat pada gambar 5.7, gambar 5.8, gambar 5.9 berikut :



Gambar 5.7 Pembangkitan kunci file pengujian1

c. Mencatat kunci publik, kunci privat serta elemen pembangun dari hasil pembangkitan kunci menggunakan bilangan prima mersenne. Hasil dari pengujian bilangan prima mersenne pada Algoritma

Elgamal dapat dilihat pada table 10.1 berikut :

Tabel 10.1 Hasil pembangkitan bilangan prima

Bilangan prima	Kunci public	Kunci privat	Elemen pembangun
461	434	113	432
461	176	260	432
461	43	321	432

Untuk melihat hasil enkripsi dari penggunaan kunci publik maka harus keluar dari menu log activity.

d. Hasil enkripsi ketiga file akan terlihat ketika menu log activity ditutup. Tampilan antar muka file pengujian yang telah dienkrip terdapat pada gambar 5.10, gambar 5.11, gambar 5.12 berikut :

KESIMPULAN

1. Algoritma Elgamal mempunyai dua kunci untuk mengamankan file.txt yaitu kunci public dan kunci privat, jika dilihat dari pengujian sistem dengan penginputan bilangan yang sama dan dilakukan proses berulang-ulang maka kunci privat dan kunci publik yang didapatkan juga berbeda – beda, sehingga untuk penebakan bilangan kunci dengan mersenne ini sangat sulit
2. Ukuran file yang belum dienkripsi lebih kecil dari file yang telah dienkripsi
3. Pengimplemnetasian kriptografi elgmala dengan mersenne sangat tepat menggunakan pemrograman java karena pemrograman java type datanya dapat menampung bilangan tertertinggi dari prima mersenne

DAFTAR PUSTAKA

Richard A Mollin, 2007. An Introduction Crytography 2nd Ed. Chapman & Hall/CRC. London. 181-182.

Mayor Lek Imat Rakhmat Hidayat dan Mayor Lek Budianto, 2011. Penghematan waktu Eksekusi Generator Bilangan prima menggunakan Struktur Bit-Array. (dalam Journal of Defense Science and Technology).29

M.Taufik Tamam, dkk , 2010. Penerapan Algoritma Kriptografi Elgama untuk Pengaman File Citra. (dalam Jurnal EECCIS Vol. IV). 9 – 10.

Darkin, 1994 dalam http://digilib.unimus.ac.id/files/disk1/23/jtptunimus-gdl-s1-2008-bisrinadhi-1122-2-bab2.pdf

Kusrini, 2006. Sistem Pakar Teori dan Aplikasi. ANDI, Yogyakarta.

M. Arhami, 2005. Konsep Dasar Sistem Pakar. ANDI, Yogyakarta. 14.

Siswanto, 2010. Kecerdasan Tiruan. Graha Ilmu. Jakarta 118, 123.

Sri Kusumadewi, 2003. Artificial Intelligence (Teknik dan Aplikasinya. Graha Ilmu, Yogyakarta 113

H. Oemar Bakry,1981. Tafsir Rahmat, MUTIARA. Jakarta.

Tim Penerbit ANDI, 2009. Pengembangan Sistem Pakar Menggunakan Visual Basic. CV. ANDI OFFSET. Yogyakarta. 14 .

T. Sutojo dkk. 2011. Kecerdasan Buatan. ANDI, Yogyakarta. 13.