BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan sistem informasi banyak sekali memberikan keuntungan dalam kehidupan sehari-hari, selain itu ada juga aspek-aspek dari sisi negatif dari kemajuan sistem informasi tersebut. Hampir semua aspek masyarakat menggunakan sistem informasi berbasis komputer, apalagi informasi-informasi mudah didapat dengan adanya jaringan komputer dan internet yang menyediakan infromasi secara tepat dan akurat.

Pengiriman data atau penyimpanan data melalui jaringan komputer memerlukan suatu proses yang dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut.Proses pengiriman data yang dilakukan pada jaringan komputer publik, pada dasarnya tidak melakukan pengamanan terhadap konten dari data yang dikirim, sehingga ketika dilakukan penyadapan pada jalur pengirimannya maka data yang dapat disadap dapat langsung dibaca oleh penyadap (Ariwibowo, 2008).

Untuk menghindari kemungkinan data yang disadap dapat langsung dibaca oleh penyadap, maka data yang dikirim diacak dengan menggunakan metode penyandian tertentu sehingga pesan yang terkandung dalam data yang terkirim tersebut menjadi lebih aman. Namun, hanya dengan menyandikan pesan tersebut, tidak menutup kemungkinan pesan dirubah oleh pihak ke tiga. Untuk memperkuat kerahasiaan serta keaslian dari pesan tersebut, maka berkembanglah tanda tangan digital. Penerima pesan akan percaya bahwa pesan yang dikirimkan masih otentik, karena telah dibubuhkan tanda tangan pada pesan tersebut. Selanjutnya, untuk mengatasi permasalahan di atas, dapat diselesaikan dengan kiptografi. Kriptografi tidak hanya menyediakan alat untuk keamanan pesan, tetapi juga sekumpulan teknik yang berguna (Rinaldi, 2006).

Menurut Doni Ariyus (2008), kriptografi didefinisikan sebagai ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) dengan cara

menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna bagi yang tidak memahaminya.

Banyak jenis tentang algoritma kriptografi untuk mengamankan pesan rahasia. Salah satu algoritma yang digunakan dalam mengamankan data pesan yaitu menggunakan algoritma ElGamal. Algoritma ElGamal termasuk dalam kategori algoritma asimetris. Dimana dalam pembuatan algoritma tersebut didapat dua kunci yaitu kunci publik dan kunci rahasia.

Algoritma tersebut pertama kali dikembangkan oleh Taher ElGamal pada tahun 1985. Sampai saat ini, algoritma ElGamal masih dipercaya sebagai metode penyandian,seperti pada pengamanan *e-mail* dan tanda tangan digital. Pada tahun 1994 pemerintah Amerika Serikat mengadopsi *Digital Signature Standard*, sebuah mekanisme penyandian berdasar pada algoritma ElGamal (Massandy, 2009).

Keamanan algoritma ElGamal terletak pada kesulitan penghitungan logaritma diskrit pada bilangan modulo prima yang besar sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sangat sukar. Pada sistem ElGamal pembentukan kunci dilakukan dengan memilih secara acak bilangan prima p yang bernilai besar dan mencari nilai α yang merupakan elemen primitif dari grup $Z_p *$. Kemudian mencari bilangan bulat a secara acak, $1 < a < p - 2$ dimana$a$ merupakan kunci rahasia dan menghitung $\beta = \alpha^a \ mod \ p$ (Joseph and Penzhorn. 2003).

Untuk mengenkripsikan pesan m, $0 < m < p - 1$, diambil sebarang bilangan acak rahasia $k \in \{0, 1, \dots, p - 2\}$. Teks kode diekspresikan dengan dua penanda (γ_i, δ_i)yaitu $\gamma_i = \alpha^{k_i} (mod \ p)$ dan $m_i = \delta_i . \gamma_i^{p-1-a} \ mod \ p$.

Berdasarkan latar belakang masalah diatas maka penulis memilih judul "Pengamanan Data Pesan Menggunakan Algoritma ElGamal".

1.2 Rumusan Masalah

Berdasarkan pada latar belakang diatas, maka rumusan masalah dalam penelitian ini adalah

1. Bagaimana membangkitkan bilangan acak (prima atau tidak prima) untuk menjadi kunci dalam sistem algoritma ElGamal?
2. Bagaimana menyandikandan membubuhkan tanda tangan digitalpada suatu data pesan dengan menggunakan konsep matematis yang ada pada algoritma ElGamal ?

1.3 Batasan Masalah

Pada penelitian ini, pembahasan algoritma ElGamal hanya meliputi :

1. Konsep matematis yang menjadi dasar dalam pembentukan dan proses penyandian suatu data pesan serta pemberian tanda tangan digital pada pesan tersebut.
2. Data yang akan disandikan pada penelitian ini hanya data berupa teks.
3. Pada penelitian ini tidak dibahas bagaimana sulitnya memecahkan mekanisme penyandian tersebut.

1.4 Tujuan Penelitian

Selain untuk memenuhi syarat kelulusan program Strata-1 (S1) Program Studi Matematika Universitas Negeri Medan, penelitian ini bertujuan:

1. Membangkitkan bilangan acak (prima atau tidak prima) untuk menjadi kunci dalam sistem algoritma ElGamal.
2. Menyandikandan membubuhkan tanda tangan digital pada suatu data pesan dengan menggunakan konsep matematis yang ada pada algoritma ElGamal.

1.5 Manfaat Penelitian

Adapun manfaat penelitian dari pembahasan masalah ini adalah sebagai berikut :

1. Manfaat bagi Penulis

   Untuk memperdalam dan mengembangkan wawasan disiplin ilmu yang telah dipelajari untuk mengkaji permasalahan tentang Pengamanan Data Pesan Menggunakan Algoritma ElGamal.

2. Manfaat bagi Pembaca

   Sebagai tambahan wawasan dan informasi tentang implementasi algoritma ElGamal dalam pengamanan informasi dan dapat dijadikan acuan dalam pengembangan penulisan karya tulis ilmiah.