BAB I

PENDAHULUAN

1.1 Latar Belakang

Surat menyurat adalah salah satu metode untuk berkomunikasi antara individu, kelompok atau organisasi maupun instansi baik dalam desa, kota, provinsi bahkan negara. Surat menyurat bisa berbentuk tulisan, gambar maupun audio visual. Akan tetapi perkembangan teknologi semakin maju, di mana surat yang dulunya di kirimkan dengan jasa pengiriman seperti POS Indonesia seketika berubah dengan munculnya elektronik mail atau biasa di sebut e-mail. E-mail tersebut konsepnya sama dengan jasa pengiriman tetapi e-mail berbentuk elektronik di mana pengirim dan penerima melakukan surat menyuratnya menggunakan media elektronik, seperti handphone, komputer dan media perangkat elektronik lainnya.

Namun pada kenyataanya kenyamanan bertolak belakang dengan keamanan, seperti yang di alami oleh perusahaan yang bergerak di komoditi furniture dan spare-part kendaraan di Jakarta, PT Primadaya Indotama yang dimuat di website www.antarnews.com pada 20 Januari 2014, di mana perusahaan tersebut melakukan kerja sama dengan perusahaan Singapura, United Impact PTE LTD dalam hubungan bisnis metal dan logam. Pelaku pembajakan e-mail perusahaan tersebut, melakukan penipuan dengan menggunakan alamat e-mail seolah-olah sama kepada perusahaan Singapura ini dengan instruksi supaya pembayaran dikirim ke nomor rekening tertentu. Hal ini juga di alami oleh presiden Meksiko yaitu Enrique Pena Nieto di mana e-mail yang digunakan

sebulan sebelum Enrique Pena Nieto terpilih menjadi presiden yang berisi nama-nama yang akan menjabat di pemerintahannya, di mata-matai oleh *National Security Agency* (NSA) dimuat di www.international.sindonews.com pada 2 September 2013.

Itu sebabnya perlunya pengamanan terhadap surat tersebut dengan cara mengenkripsi atau merubah isi surat menjadi tidak sesuai aslinya, tujuannya untuk menghindari penyadapan surat oleh orang yang tidak bertanggung jawab. Agar isi surat hanya bisa dibaca oleh pengirim dan penerima, isi surat terlebih dahulu di enkripsi dengan algortima kriptografi dan penerima membaca isi surat dengan terlebih dahulu mendekripsi menggunakan algortima kriptografi, apabila ada pihak lain yang melakukan penyadapan atau pengambilan data, orang tersebut kebingungan membaca isi surat tersebut.

Penulis mengusulkan sebuah aplikasi e-mail client yang menerapkan algoritma ElGamal. Diharapkan hasil akhir dari aplikasi yang dibangun ini dapat bermanfaat bagi para pengguna yang menginginkan surat elektroniknya terjamin.

1.2 Rumusan Masalah

Keamanan data merupakan suatu hal yang harus ada untuk memberikan kenyamanan, apalagi jika isi surat tersebut bersifat rahasia. Berdasarkan uraian latar belakang di atas, penulis mengidentifikasi beberapa hal yang menjadi rumusan permasalahan :

1. Bagaimana mengetahui cara kerja algoritma ElGamal?
2. Bagaimana implementasi algoritma ElGamal pada aplikasi enkripsi teks untuk aplikasi e-mail client?

1.3 Ruang Lingkup

Dalam penulisan tugas akhir ini penulis akan membatasi masalah pada beberapa hal berikut ini :

1. Metode Kriptografi yang digunakan yaitu ElGamal.
2. Kunci yang digunakan hanya kunci asimetri.
3. Informasi yang akan di enkripsi hanya berupa teks.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui cara kerja Algoritma ElGamal.
2. Mengimplementasikan algoritma ElGamal pada aplikasi enkripsi teks untuk e-mail client.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini ialah sebagai berikut :

1. Membantu pengguna e-mail dalam memperlancar surat menyuratnya dengan melakukan pengamanan antar pengirim dan penerima.
2. Terhindar dari ancaman penyadapan e-mail.