BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang pesat mempengaruhi kehidupan manusia, manusia dapat melakukan berbagai kegiatan yang ada sekarang hanya melalui perangkat yang terhubung melalui internet, seperti melakukan pembayaran listrik, melakukan transfer, mengisi uang elektronik, bertukar kabar dan lain-lain. Namun, informasi yang mengalir di ponsel pintar atau internet tidaklah menjamin keamanan data penggunanya. Karena siapapun dapat menggunakan internet, maka sangat rentan terhadap penyadapan oleh pihak yang tidak berkepentingan...[1].

Untuk memastikan suatu data terjamin keamanannya maka diperlukan beberapa persyaratan yaitu harus ada yaitu *Confidentiality*, *Integrity*, dan *Availability* (*CIA*). *Confidentially* (kerahasiaan) dapat dideskripsikan sebagai dasar bahwa informasi yang ada tidak akan tersedia atau diungkapkan kepada orang lain. Data harus dijaga dari kebocoran oleh orang yang tidak berkepentingan. Integritas berkaitan dengan keakuratan dan kelengkapan data dan informasi. Data dan informasi yang ada harus disimpan dalam bentuk yang benar, dan tidak seorang pun dapat mengubahnya jika tidak benar, meskipun itu kecelakaan atau niat untuk melakukan kejahatan. Tujuan dari integritas berdasarkan desain adalah untuk melindungi data agar tidak dihapus atau diubah oleh orang yang tidak berwenang, dan untuk memastikan bahwa ketika orang yang berwenang membuat perubahan, perubahan tersebut dapat dibatalkan.

Availability (Ketersediaan) berfungsi agar pengguna yang berkepentingan dengan suatu data dapat mengakses data tersebut dengan mudah dimanapun dan kapanpun diperlukan. Tidak hanya data dan informasi, tetapi juga metode otentikasi, metode akses dan sistem manajemen harus bekerja secara efektif untuk melindungi data dan informasi yang terkandung di dalamnya, dan untuk menjamin ketersediaan data dan informasi tersebut sesuai kebutuhan. [2]. Ketika beberapa data pribadi dibagikan di media sosial, pengguna menjadi subjek uji serangan seperti spam, malware, bot sosial, dan pencurian identitas. Sedangkan

peretas dapat menemukan data penting lainnya seperti informasi rekening bank yang dapat digunakan untuk kejahatan seperti penipuan, lalu identitas dan lokasi. Masalah keamanan merupakan salah satu aspek penting yang ada di internet. Sayangnya masalah keamanan ini kurang mendapat perhatian bagi para pengguna internet, masalah keamanan data privasi selalu di urutan kedua, atau bahkan terakhir dalam daftar hal-hal yang dianggap penting [16].

Algoritma ElGamal dikenal sebagai kriptosistem asimetris yang sangat kuat dalam hal enkripsi dan dekripsi yang ditemukan pada tahun 1985 oleh Taher ElGamal. ElGamal menyajikan bentuk yang sama untuk mengenkripsi dalam penerapan kunci publik dan kunci pribadi. Algoritma ini mewakili metode alternatif untuk cipher kunci publik RSA, keamanan ElGamal bergantung pada kesulitan menghitung modulus logaritma diskrit dari bilangan prima yang besar. Memecahkan sistem kriptografi ini hampir tidak mungkin tercapai atau membutuhkan waktu yang sangat lama. Keuntungan dari teknik ElGamal adalah bahwa pesan teks biasa yang sama menghasilkan pesan teks sandi yang berbeda setiap kali dienkripsi [4].

Tidak semua yang dibicarakan di Internet bersifat publik, dan banyak orang mengetahuinya. Ada kalanya suatu hal dibagikan sehingga hanya orang-orang tertentu saja yang mengetahuinya. Tentu saja, jika pesannya bersifat rahasia, sulit untuk mencegat pesan yang dikirim selama percakapan. Oleh karena itu, untuk melindungi dan menjaga privasi data, jauhkan dari orang yang tidak mempunyai hak untuk mengakses informasi tersebut, yaitu dengan menggunakan metode enkripsi. Kriptografi adalah ilmu dan seni menjaga kerahasiaan pesan dengan menyandikannya sehingga tidak dapat dimengerti [16].

1.2 Rumusan Masalah

Dari latar belakang yang sudah dipaparkan di atas, masalah yang akan dibahas padapenelitian ini adalah:

1. Bagaimana mengimplementasikan ElGamal pada aplikasi pengiriman pesan?
2. Bagaimana meningkatkan keamanan pada aplikasi pengiriman pesan dan berapa besar dampak peningkatan keamanan tersebut dari sisi *computational cost*?

1.3 Batasan Masalah

Penelitian ini dilakukan untuk meningkatkan keamanan pertukaran data pada aplikasi Pengiriman Pesan menggunakan algoritma ElGamal. Perangkat yang digunakan yaitu berupa aplikasi windows dimana hasil akhirnya berupa nilai yang menunjukan seberapa baik penerapan ElGamal pada aplikasi pengiriman pesan dalam mengamankan data dan seberapa efisien dalam melakukan enkripsi.

1.4 Tujuan

Penelitian ini bertujuan untuk:

1 Mengimplementasikan algoritma ElGamal pada aplikasi pengiriman pesan

2 Meningkatkan keamanan pada aplikasi pengiriman pesan dan berapa besar dampak peningkatan keamanan tersebut dari sisi *computational cost.*

1.5 Rencana Kegiatan

Rencana Kegiatan yang dilakukan pada penelitian ini adalah sebagai berikut:

1. Studi Literatur

   Studi literatur merupakan bagian awal dalam pengerjaan Tugas Akhir. Kegiatan yang terdapat pada studi literatur antara lain mencari, membaca, serta memahami pustakayang berkaitan dengan topik ElGamal.

2. Perancangan Sistem

   Perancangan sistem merupakan implementasi algoritma ElGamal untuk meningkatkan keamanan data. Menggunakan aplikasi Visual Studio Code menggunakan bahasa *Phyton*.

3. Pengujian Sistem

   Dari mengimplementasikan algoritma *ElGamal* untuk meningkatkan keamanan data. Pengujian sistem dilakukan menggunakan 3 skenario uji, pertama pengujian tingkat keamanan sistem dengan simulasi penyerangan menggunakan MITM, kedua pengujian *computational cost* dibagi jadi 2 yaitu *time cost* dan *memory cost*.

4. Evaluasi Hasil

   Setelah dilakukan pengujian aplikasi yang telah dibangun didapatkan hasil pengujian untuk mengetahui bagaimana peningkatan keamanan dan bagaimana hasil *computational cost*.

5. Penulisan Laporan

   Dokumentasi laporan mengenai hasil akhir dari penelitian yang telah dilakukan dalam laporan pengerjaan tugas akhir.