BAB 1
PENDAHULUAN

1.1 Latar Belakang

Era digital seperti saat ini keamanan data menjadi salah satu hal yang sangat penting karena semakin banyaknya aktivitas dan interaksi yang di lakukan secara *online*. Khususnya dalam mengirimkan pesan, terutama pesan teks dalam bentuk dokumen. Dokumen adalah salah satu alat untuk menyampaikan pernyataan ataupun informasi melalui tulisan, dari satu pihak ke pihak lainnya.

Teks merupakan suatu ungkapan berupa tulisan yang memiliki isi serta makna yang menjadi sebuah penjelasan akan sebuah hal. Pesan digital teks merupakan suatu data/informasi berupa tulisan yang diolah dan diberikan oleh pengirim menggunakan suatu teknologi yang dibuat bertujuan agar penerima tahu yang disampaikan oleh pengirim.

Ancaman terhadap pengamanan data akan semakin meningkat, ketika data yang di proses dalam sebuah teknologi semakin banyak. *Doc.x* adalah salah satu format *file* yang ada pada aplikasi *Microsoft Office*. Umum digunakan oleh pengguna komputer sebagai aplikasi pengolah kata. *File* berekstensi (*.docx) pertama kali hadir pada *Microsoft Office Word* 2007. Format jelas ini memiliki keunggulan di bandingkan format sebelumnya. Maka sangat memungkinkan untuk mengirimkan informasi menggunakan *file* docx. Namun karena tingkat keamanannya rendah, jadi sangat beresiko apabila mengirimkan data atau konten teks berbasis dokumen yang sifatnya rahasia.

Dalam Al-Qur'an Allah juga menjelaskan bahwa Ia Maha Menjaga Keamanan. Dalam konteks ini sangat erat kaitannya dengan penelitian in. Karena penelitian ini juga bertujuan untuk menjaga keamanan data teks yang mungkin sangat diperlukan perusahaan atau individu.

وَالَّذِينَ هُمْ لِأَمَانَاتِهِمْ وَعَهْدِهِمْ رَاعُونَ

Dan orang-orang yang memelihara amanat-amanat (yang dipikulnya) dan janjinya. (QS.Al-Mu'minun:8).

Dari ayat diatas penulis mengambil kesimpulan bahwa orang-orang mukmin haruslah menjaga setiap amanat yang diberikan kepadanya. Baik harta, perabuatan dan perkataan (pesan) yang dalam era digital sekarang erat kaitannya dengan penyampain informasi berupa teks melalui sistem online, maka dari itu untuk menjaga keaslian dari sebuah pesan dan dokumen perlu ada pengamanan data melalui ilmu kriptografi.

Kriptografi adalah pembelajaran matematis dengan aspek- aspek berkaitan dengan keamanan informasi seperti menyembunyikan data, mencegah perubahan data tanpa terdeteksi dan mencegah data digunakan tanpa izin. Kriptografi dilakukan untuk menyembunyikan konten dari suatu informasi menjadi sandi dengan menggunakan kunci dan untuk membacanya juga diperlukan kunci pula. Algoritma *prime generator* Fermat ditemukan oleh seorang matematikawan asal Prancis bernama Pierre de Fermat pada abad ke-17. Beliau mengemukakan penemuannya mengenai hubungan bilangan prima dengan aritmatika modular. Dengan munculnya teorema ini memberikan peranan yang sangat penting dalam menentukan nilai bilangan prima.

Algoritma ElGamal adalah algoritma asimetris yang dibuat oleh Taher ElGamal pada tahun 1985. Algoritma ini mempunyai kelebihan yang terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan algoritma ini tergolong sulit. Dengan menggunakan logaritma diskrit dengan metode enkripsi dan dekripsi pada proses komputasi yang besar ini menjadikan enkripsinya menjadi lebih besar berkali lipat dari ukuran sebelumnya, ini merupakan kelebihan dari algoritma ElGamal. ElGamal juga digunakan dalam perangkat lunak *security* yang dikembangkan oleh GNU, program PGP, dan pada sistem keamanan lainnya. Berdasarkan uraian diatas, penulis tertarik untuk mengajukan tugas akhir yang berjudul : "**Pengamanan Data Teks Berbasis Dokumen Menggunakan Algoritma *Prime Generator* Fermat dan Algoritma ElGamal".**

1.2. Rumusan Masalah

Rumusan masalah dari penelitian ini adalah bagaimana merancang sistem keamanan data teks berbasis dokumen dengan mengkombinasikan Algoritma *Prime Generator* Fermat dan Algoritma ElGamal.

1.3. Batasan Penelitian

Dalam pembuatan tugas akhir ini, untuk mengatasi permasalahan yang ada maka penyusun membatasi permasalahan sebagai berikut :

1. Data yang digunakan adalah *file* dengan ekstensi (*.docx) dan hanya mengenkripsi berupa *string*, tidak tabel dan gambar .
2. Hanya satu file yang digunakan dalam implementasi dan pengujian.
3. Menggunakan Algoritma Prime *Generator* Fermat dan Algoritma ElGamal.
4. Menghitung waktu eksekusi & jumlah *ciphertext, plaintext.*
5. Karakter yang digunakan pada *plaintext* dan *ciphertext* adalah kode ASCII (*American Standart Code for Information Interchange*) 256 (8 bit).
6. Bahasa pemrograman yang digunakan adalah C#.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah mengimplementasikan dua kombinasi metode kriptografi antara Algoritma *Prime Generator* Fermat dan Algoritma ElGamal untuk mengamankan data string berekstensi *.docx* .

1.5. Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah :

1. Mengetahui bagaimana langkah-langkah mengamankan data string berekstensi *.docx* dengan menerapkan dua kombinasi: Algoritma *Prime Generator* Fermat dan Algoritma ElGamal.
2. Apabila dipublikasikan, aplikasi yang telah dirancang dalam penelitian ini dapat memudahkan beberapa pengguna untuk kebutuhan tertentu.
3. Merancang sistem untuk mengamankan data.
4. Referensi bagi peneliti lain yang ingin meneliti topik penelitian sama.