BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Untuk menjaga keamanan yang mempunyai informasi-informasi rahasia penting, maka digunakanlah salah satu teknik pengaman informasi dengan menggunakan algoritma penyandian data. Pada sistem ini akan menggunakan algoritma penyandian data/kriptografi ElGamal yang akan diimplementasikan pada sebuah aplikasi. Menurut jurnal *A Public Key Cryptosystem and a SignatureScheme Based on Discrete Logarithms* menyebutkan bahwa kekuatan Algoritma Kriptografi Elgamal terletak pada kalkulasi tanda tangan digital yang menekankan pada perhitungan algoritma diskrit sehingga tanda tangan digital atau kunci rahasia tersebut tidak dapat di kriptalis. Mengingat penting pengaman tersebut, maka mengangkat judul tugas akhir yaitu "**Implementasi Algoritma Kriptografi ElGamal Pada Data Text**". Sehingga dengan dibuatnya tugas akhir ini dapat mempermudah pengguna dalam mengamankan sebuah informasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang permasalahan pada subbab ini maka masalah-masalah yang ada dapat dirumuskan sebagai berikut:

Bagaimana merancang aplikasi untuk keamanan data dengan menggunakan metode Algoritma Kriptografi ElGamal ke dalam sebuah Aplikasi.

1.3 Tujuan Penelitian

Dapat membuat suatu aplikasi untuk keamanan dengan menggunakan metode Algoritma Kriptografi ElGamal.

1.4 Batasan Masalah

Dalam Tugas Akhir ini ruang lingkup permasalahannya hanya akan dibatasi pada :

1. Implementasi dilakukan pada program desktop.
2. Metode yang digunakan untuk kriptografi adalah Algoritma Kriptografi Elgamal.
3. Hanya dapat digunakan pada file berekstensi .txt dan ekstensi khusus yang dibuat oleh penulis.

1.5 Manfaat Penelitian

Manfaat dalam pembuatan aplikasi ini adalah membantu dalam mengamankan suatu informasi agar terhindar dari penyadapan atau penyalahgunaan.

1.6 Metodelogi Penelitian

Metode yang digunakan dalam pembuatan aplikasi ini adalah :

1. Tempat dan Waktu Penelitian

   Tempat : Malang

   Wilayah : Malang

   Waktu Penelitian :

2. Studi Pustaka

Untuk mendukung pembuatan sistem aplikasi ini, dilakukan studi pustaka dengan mengumpulkan bahan dari beberapa sumber, seperti media internet, jurnal-jurnal, dan beberapa buku referensi yang membahas tentang metode Algoritma Kriptografi ElGamal beserta fasilitas pendukungnya.

3. Data Perancangan Sistem

Penelitian dilakukan dengan mengumpulkan referensi mengenai metode yang digunakan dalam Algortima Kriptografi ElGamal beserta fasilitas pendukungnya.

4. Langkah Perancangan Sistem

a. Studi Pendahuluan

Melakukan studi pendahuluan dan analisis mengenai hal-hal yang berkaitan dengan penyelesaian masalah dan pembuatan sistem aplikasi. Seperti rumus, teknik, cara kerja yang dibutuhkan dalam pembuatan program.

b. Analisis dan Perancangan Sistem

Merancang sistem aplikasi dengan menggunakan metode Algortima Kriptografi ElGamal, yang dapat dimengerti serta dapat dioperasikan.

c. Pembuatan Program

Mengimplementasikan hasil rancangan sistem ke dalam bahasa pemrograman.

Klasifikasi perangkat keras yang digunakan adalah :

- Intel Core 2 Duo –T7500 2.2 GHz
- Memory DDR2 2 GB
- VGA Intel GMA X3000
- Hard Disk 160 GB
- DVD-RW Mashita8X

Sedangkan perangkat lunak yang digunakan adalah :

- Sistem Operasi Windows
- Microsoft Office
- Dan pendukung lainnya

d. Kesimpulan

Menyimpulkan hal-hal yang dapat mempengaruhi hasil perancangan sistem.

1.7 Sistematika Penulisan

BAB I : **Pendahuluan**

Berisi tentang latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, metodologi, dan sistematika penulisan.

BAB II: **Landasan Teori**

Menjelaskan mengenai teori-teori yang mendukung dan digunakan sebagai dasar dalam memecahkan masalah, teori-teori tersebut

diambil dari literatur yang sesuai dengan permasalahan yang dihadapi sebagai sarana pendukung dari tugas akhir.

BAB III : **Analisa Dan Perancangan**

Membahas langkah-langkah yang harus dilakukan dalam mendesain suatu sistem pengambilan keputusan yang meliputi desain flowchart, analisa pemecahan masalah.

BAB IV : **Implementasi Dan Pembahasan**

Menjelaskan tentang kebutuhan software dan hardware yang digunakan, ujuk kerja sistem, dan pembahasan.

BAB V: **Penutup**

Kesimpulan dan saran.