BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Dalam era teknologi informasi, keamanan data benar-benar menjadi permasalahan yang sangat penting. Perkembangan sistem komputer dan interkoneksinya melalui jaringan telah meningkat, tentu saja hal ini membutuhkan keamananan data dan pesan yang handal agar terhindar dari serangan (*attack*). Untuk mengamankan data atau pesan di jaringan diperlukan kriptografi dengan metode enkripsi.

Saat ini komputer hampir dapat dijumpai di setiap kantor pemerintah, perusahaan, sekolah, atau bahkan rumah tangga. Perkembangan teknologi komputer yang pesat, khususnya di bidang perangkat lunak, membuat computer menjadi semakin user friendly dan telah menjadikannya suatu kebutuhan bagi kalangan tertentu, misalnya kalangan bisnis. Dalam melakukan pekerjaan mereka sangat tergantung pada komputer. Komputer tidak lagi hanya digunakan sebagai pengganti mesin tik ataupun alat hitung, namun kini juga banyak digunakan dalam membantu pembuatan keputusan penting. Akibatnya, informasi yang disimpan memerlukan pengamanan yang dapat melindungi terhadap akses orang yang tidak berhak.

Salah satu cara yang dapat dilakukan untuk melindungi informasi tersebut adalah dengan menggunakan enkripsi.

Kriptografi telah menjadi bagian penting dalam dunia teknologi informasi saat ini. Hampir semua penerapan teknologi informasi menggunakan kriptografi sebagai alat untuk menjamin keamanan dan kerahasiaan informasi. Karena itu pulalah, kriptografi menjadi ilmu yang berkembang pesat. Dalam waktu singkat, amat banyak bermunculan algoritma-algoritma baru yang dianggap lebih unggul daripada pendahulunya.

Maka dari semua penjelasan tersebut penulis berkeinginan untuk membuat sebuah aplikasi untuk mengenkripsi plaintex dengan menggunakan algoritma *Elliptic Curve Cryptosystem* (ECC).

1.2 RUMUSAN MASALAH

Yang menjadi permasalahan dalam tugas akhir ini adalah "Bagaimana mengimplementasikan Algoritma *Elliptic Curve Cryptosystem* dalam sebuah kriptografi dengan menggunakan kunci Asimetris

1.3 BATASAN MASALAH

Yang menjadi batasan masalah dalam penelitian ini adalah :

1. Penerapan enkripsi dan dekripsi hanya pada file yang berekstensi text.
2. Algoritma yang di gunakan dalam pembuatan aplikasi ini adalah menggunakan algoritma *Elliptic Curve Cryptosystem* (ECC).
3. Bahasa pemogroman yang dipakai adalah Visual Basic 6.0.
4. Kunci yang digunakan adalah kunci asimetris.

1.4 TUJUAN PENELITIAN

Yang menjadi tujuan dalam penelitian yang akan dibangun adalah :

1. Untuk membangun sebuah sistem aplikasi yang mempunyai kemampuan mengenkripsi plaintext menjadi chiptertext dan mendekripsikan chiptertext menjadi plaintext awal.
2. Memahami cara kerja algoritma *Elliptic Curve Cryptosystem* (ECC) ke dalam aplikasi sistem.

1.5 MANFAAT PENELITIAN

Manfaat dari penelitian ini adalah:

1. Dapat membantu user untuk menggunakan data file yang berekstensi text.

2. Memahami kriptografi dengan kunci asimetris dengan menggunakan algoritma *Elliptic curve cryptosystem.*

1.6 RELEVANSI

Diharapkan dari penelitian ini dapat memudahkan seseorang dalam mengenkripsi text dan memahami cara kerja *Elliptic curve cryptosytem* (ECC) dengan baik.