BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Data merupakan sesuatu yang harus dijaga, terutama kerahasiaan dan keamanannya. Salah satu cara mengamankan data adalah menggunakan teknik kriptografi. Kriptografi merupakan salah satu metode pengamanan data yang biasa digunakan untuk menjaga kerahasiaan data, keaslian data, serta autentikasi sang pengirim pesan.

Kriptografi adalah ilmu yang berguna untuk mengacak data sedemikian rupa sehingga tidak bisa dibaca oleh pihak ketiga, data yang diacak hanya bisa dibaca oleh pihak yang berwenang dengan menggunakan sebuah kunci yang sudah disepakati.

Data yang ingin diacak biasa disebut plainteks dan di enkripsi menggunakan kunci enkripsi, data hasil enkripsi dinamakan chiperteks dan di dekripsi kembali menggunakan kunci dekripsi.

Dari segi algoritma yang digunakan, kriptografi dibagi menjadi 2, algoritma kunci simetri dan asimetri. Pada algoritma kunci simetri, kedua pihak menggunakan kunci umum yang sama, sedangkan pada algoritma kunci asimetri, kedua pihak masing-masing berbagi kunci publik.

Algoritma kriptografi yang baik membutuhkan waktu yang lama untuk memecahkan pesan yang telah disandikan. Seiring dengan berkembangnya teknologi komputer, dunia teknologi membutuhkan algoritma kriptografi yang lebih kuat dan aman.

Algoritma *AES* atau *Rijndael* adalah salah satu contoh algoritma kunci simetris, diciptakan oleh Vincent Rijmen dan John Daemen asal Belgia sebagai pemenang kompetisi kriptografi untuk mencari pengganti *DES* yang diselenggarakan oleh *NIST* (*National Institute of Standards and Technology*) pada tahun 2001. Setelah mengalami proses standarisasi oleh *NIST*, akhirnya pada bulan Mei 2002 *Rijndael / AES* ditetapkan sebagai standar algoritma kriptografi.

1.2 RUMUSAN MASALAH

Bagaimana membuat program yang mengimplementasikan algoritma *AES* agar bisa digunakan untuk mengamankan data berbasis teks agar tidak bisa dibaca oleh pihak yang tidak berwenang.

1.3 TUJUAN

Membuat sebuah program yang bisa digunakan untuk mengamankan data dengan menggunakan kriptografi algoritma *AES*.

1.4 PEMBATASAN MASALAH

- Data yang diamankan / diacak berupa data berbasis teks saja
- Program dibuat menggunakan bahasa pemgograman C#
- Program dibuat menggunakan Microsoft Visual Studio C#
- Kapasitas maksimal input sama dengan kapasitas maksimal textbox program yang digunakan

1.5 SISTEMATIKA PENULISAN

BAB I PENDAHULUAN

Berisikan tentang latar belakang masalah dan tujuan dibuatnya karya tulis ini.

BAB II LANDASAN TEORI

Berisikan tentang teori – teori mengenai kriptografi, macam – macam algoritma kriptografi, algoritma *AES / Rijndael* dan beberapa serangan terhadap teknik kriptografi

BAB III PERANCANGAN

Berisi tentang bagaimana jalannya program yang mengimplementasikan Algoritma *AES / Rijndael*

BAB IV PENGAMATAN DATA

Berisi tentang hasil keluaran program dan beberapa percobaan

BAB V Kesimpulan dan Saran

Berisi kesimpulan dan saran

Pada akhir laporan ini akan diikuti daftar pustaka dan lampiran.