BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Data dapat menjadi salah satu aset penting dalam kelangsungan hidup perusahaan manapun. Salah satu cara untuk untuk mengamankannya dari kejahatan orang lain adalah mengenkripsinya. Kriptografi adalah ilmu yang mempelajari bagaimana suatu pesan atau dokumen kita aman, tidak bisa dibaca oleh pihak yang tidak berhak. Dalam perkembangannya, kriptografi juga digunakan untuk identifikasi pengirim pesan dengan tanda tangan digital dan keaslian pesan dengan sidik jari digital (fingerprint). Kriptografi mempunyai se jarah yang sangat panjang. Sejak jaman Romawi, Julius Caesar telah menggunakan teknik kriptografi yang sekarang dianggap kuno dan sangat mudah dibobol untuk keperluan komunikasi militernya. Namun sekutu dapat menembus Enigma, kriptografi produk Jerman dan Purple,kriptografi produk Jepang, sekutu akhirnya dapat memenangkan perang dunia kedua karena dapat mengetahui beberapa langkah dan strategi militer lawan. Dalam hal teknik pengamanan data, banyak metoda kriptografi yang dapat digunakan. Metode – metode kriptografi tersebut mempunyai teknik dan cara tersendiri. Langkah – langkah pengerjaan setiap metode pun berbeda – beda, baik dari segi panjang maupun kerumitan. Algoritma kriptogenik yang digunakan pada Advanced Encryption Standard (AES) adalah algoritma *Rijndael*. Algoritma ini adalah pemenang sayembara terbuka yang diadakan oleh NIST (National Institute of Standards and Technology) pada tahun 2001. AES menggunakan blok cipher simetris untuk proses enkripsi dan dekripsi yang dapat memproses data input 128 bit dengan menggunakan chiper key 128, 192 atau 256 bit.

Pada algoritma *Rijndael*, data input atau plaintext diproses melalui serangkaian transformasi, disebut Chiper, yang terdiri dari transformasi SubBytes, ShiftRows, MixColumns dan AddRounKey, dengan menggunakan kunci kriptogenik rahasia yaitu Chiper Key. Data yang dihasilkan chiper disebut Ciphertext dan akan diproses untuk dikonversikan kembali menjadi plaintext melalui serangkaian transformasi disebut Inverse Chiper, yang terdiri dasri transformasi InvShiftRows, InvSubBytes, AddRoundKey dan InvMixColumns, dengan menggunakan chiper key.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah yang diuraikan, masalah yang dapat diidentifikasikan penulis yaitu :

1. Bagaimana cara mengenkripsi dan mendekripsi suatu data dengan menggunakan metode kriptografi Advanced Encryption Standard (AES).
2. File apa saja yang bisa dienkripsi dan dekripsi menggunakan metode kriptografi Advanced Encryption Standard (AES).
3. Bagaimana membuat suatu perangkat lunak enkripsi-dekripsi dengan menggunakan metode kriptografi Advanced Encryption Standard (AES).

1.3. Batasan Masalah

Untuk mencegah meluasnya pembahasan masalah tersebut diatas , maka ruang lingkup permasalahan akan dibatasi antara lain :

1. Algoritma yang digunakan adalah Algoritma *Rijndael*.
2. Pembuatan aplikasi dengan visual basic 6.0.
3. Tidak melakukan perbandingan kecepatan waktu proses enkripsi dan dekripsi dengan algoritma lain.

1.4. Tujuan Penelitian

Tujuan dari penyusunan tugas akhir ini adalah :

1. Membuat perangkat lunak enkripsi dan dekripsi data menggunakan metode kriptografi AES dengan bahasa pemrograman visual basic 6.0.
2. Mengetahui kekuatan algoritma *Rijndael* terhadap serangan brute force.

1.5. Sistematika Penulisan

Sistematika penulisan proposal penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I. PENDAHULUAN

Menguraikan tentang latar belakang permasalahan, identifikasi masalah, batasan masalah, tujuan penelitian, serta sistematika penulisan.

BAB II. LANDASAN TEORI

Membahas beberapa teori penunjang yang berhubungan dengan pokok pembahasan dalam Tugas Akhir ini yang secara garis besar berisi tentang pembuatan dan penerapan perangkat lunak enkripsi -dekripsi menggunakan metode AES menggunakan bahasa pemrograman Visual basic 6.0

BAB III. METODE PENELITIAN

Bab ini memberikan keterangan tentang cara dan prosedur dalam melakukan penelitian.

BAB IV. ANALISIS DAN PEMBAHASAN

Bab ini mencakup analisa dan perancangan dalam Tugas Akhir dan berbagai pengujian yang dilakukan terhadap perangkat lunak yang dikembangkan beserta hasil pengujiannya .

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang berkenaan dengan hasil pemecahan masalah yang diperoleh dari penyusunan tugas akhir ini. Serta beberapa saran untuk pengembangan lebih lanjut .