BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan data adalah usaha mengamankan data dari pengubahan maupun akses yang tidak sah. Keamanan data difokuskan untuk memastikan kerahasiaan data. Salah satu usaha penjagaan keamanan data adalah kriptografi. Pada dasarnya, kriptografi adalah ilmu dan seni untuk menjaga keamanan data, namun seiring perkembangan jaman, kriptografi juga digunakan untuk mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentifikasi (Menezes, 1996).

Keamanan data makin berkembang seiring dengan perkembangan teknologi.Hal ini disebabkan oleh banyaknya usaha manipulasi data dari pihak yang tidak berwenang. Perkembangan keamanan data ditandai dengan berkembangnya ilmu kriptografi. Seiring dengan perkembangan jaman, algoritma kriptografi kian bertambah dan beraneka ragam. Beberapa algoritma kriptografi klasik adalah *affine, vigenere,* dan *playfair*. Algoritma kriptografi klasik hanya berupa teknik substitusi dan transposisi sederhana yang cenderung dapat dipecahkan dengan mudah oleh statistik, terkaan, intuisi, dan sebagainya (Munir, 2006). Berbeda dengan algoritma kriptografi klasik, algoritma kriptografi modern dibuat sedemikian kompleks sehingga sangat sulit dipecahkan jika kunci tidak diketahui. Algoritma kriptografi modern tidak hanya memakai substitusi dan transposisi, namun rangkaian *bit*, operasi *XOR*, *stream chiper*, *block chiper*, *generated key*, *shift*, dan lain sebagainya. Beberapa algoritma kriptografi modern antara lain DES, *Rivest Code*, dan *Rijndael*.

Sejak tahun 1997, *National Institute of Standarts and Technology* (NIST) telah bekerja dengan *International Cryptographic Community* untuk pengembangan *Advanced Encryption Standart* (AES) dengan pengadaan kompetisi terbuka. Syarat yang diajukan oleh NIST untuk algoritma baru yang akan menjadi AES adalah termasuk algoritma simetri berbasis *block chiper*, panjang kunci fleksibel (128, 192, dan 256 bit), dan ukuran blok yang dienkripsi adalah 128 bit. Ada banyak algoritma yang diajukan, namun pemenangnya adalah algoritma *Rijndael* (Daemen dan Rijmen, 2003) dengan alasan algoritma lain terdapat kekurangan terhadap serangan dan performa yang tidak lebih baik daripada algoritma *Rijndael*.

Rijndael menggunakan substitusi, permutasi, transformasi, dan sejumlah perputaran.Dikarenakan banyaknya operasi yang ada dalam algoritma *Rijndael* dan

pengakuan NIST sebagai algoritma kriptografi standar AES, maka penulis berkeinginan untuk melakukan implementasi dan pengujian terhadap algoritma tersebut.Oleh karena itu judul skripsi ini adalah "**Implementasi Algoritma *Rijndael* untuk Keamanan Data**".

.

1.2 Rumusan Masalah

Rumusan masalah yang akan dijadikan objek penelitian pada skripsi ini adalah:

1. Bagaimana menerapkan algoritma *Rijndael?*.
2. Bagaimana ketahanan algoritma rijndael terhadap serangan menggunakan *exhautive attack?*

1.3 Batasan Masalah

Ruang lingkup yang membatasi permasalahan yang akan dibahas pada skripsi ini antara lain:

1. Data uji berupa file text.
2. Pengujian yang akan dilakukan adalah pengubahan kunci dekripsi.

1.4 Tujuan

Tujuan yang ingin dicapai dari pembuatan skripsi ini adalah:

1. Membangun aplikasi kriptografi yang menerapkan algoritma *Rijndael*.
2. Menghasilkan aplikasi kriptografi dengan menggunakan presentasi perbandingan *exhautive attack*.

1.5 Manfaat

Manfaat yang bisa diambil dari penyusunan skripsi ini adalah:

1. Terbangunnya aplikasi implementasi algoritma kriptografi *Rijndael* untuk keamanan data teks.

1.6 Sistematika Penulisan

Pembuatan skripsi ini dilakukan dengan pembagian bab sebagai berikut.

1. BAB I PENDAHULUAN

Pada bab ini membahas mengenai latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan.

2. BAB II KAJIAN PUSTAKA DASAR TEORI

Pada bab ini berisi teori-teori dari berbagai pustaka yang menunjang penelitian ini. Adapun teori yang tercakup dalam bab ini yaitu tentang kriptografi dan algoritma *Rijndael*.

3. BAB III METODOLOGI PENELITIAN

Bab ini berisi perancangan perangkat lunak yang akan dibangun meliputi perancangan data, perancangan proses, perancangan tabel, dan perancangan uji coba. Selain itu ada juga contoh perhitungan manual dari proses-proses yang ada.

4. BAB IV PERANCANGAN IMPLEMENTASI

Bab ini beris hasil dari implementasi perangkat lunak algoritma *Rijndael* yang digunakan untuk

5. BAB V PENGUJIAN DAN ANALISIS

Pada bab membahas tentang pengujian skripsi dan analisis penulis

6. BAB VI PENUTUP