BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan merupakan salah satu aspek penting dalam pengiriman data/informasi melalui jaringan ataupun Data pribadi dalam komputer Umum. Salah satu cara untuk menjaga keamanan dan kerahasiaan suatu data maupun informasi adalah dengan teknik enkripsi dan dekripsi. Teknik ini berguna untuk membuat pesan, data, maupun informasi tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk penerima yang berhak dan mengetahui teknik dekripsinya. Teknik enkripsi dan dekripsi dikenal dan dipelajari dalam kriptografi.

Kriptografi merupakan ilmu yang mempelajari mengenai cara mengamankan suatu informasi. Pada tahun 1990-an, algoritma enkripsi yang banyak dipakai adalah algoritma DES (*Data Encryption Standard*). Namun, seiring dengan makin canggihnya teknologi dan berkembangnya dunia *cryptanalysis,* maka keamanan data dengan algoritma DES yang menggunakan kunci sepanjang 56 bit dianggap tidak memadai lagi, karena itu pada tahun 2000 terpilihlah algoritma Rijndael sebagai standar algoritma kriptografi baru penyempurnaan algoritma DES, yang

juga dinamakan sebagai algortima AES.

Informasi berupa data rahasia seperti Pemerintahan, Militer, Badan Keuangan, Rumah Sakit, dan Perusahaan Perdagangan untuk menyimpan Informasi Penting, misalnya hasil pemeriksaan pasien dalam bidang Rumah Sakit, area geografi dalam Bidang Penelitian, posisi musuh dalam Bidang Militer, Produk baru dalam Perusahaan, dan lain sebagainya.

Melihat penting dan bermanfaatnya teknik enkripsi dan dekripsi, maka akan sangat baik pula jika metode dalam pemrosesannya menggunakan algoritma dengan besar ekspansi kunci yang tinggi, salah satunya dengan algoritma Rijndael.

Dari latar belakang di atas, maka penelitian ini akan membahas merancang dan membangun sebuah aplikasi enkripsi dan dekripsimenggunakan metode rijndael.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas diperoleh rumusan permasalahan pada penelitian ini yaitu bagaimana merancang dan membuat aplikasi enkripsi dan dekripsi, maka penelitian ini akan diberi judul APLIKASI KEAMANAN DOKUMEN-DOKUMEN DENGAN ENKRIPSI DAN dekripsiMENGGUNAKAN ALGORITMA RINJDAEL.

1.3 Ruang Lingkup

Aplikasi enkripsi dan dekripsikeamanan Adapun ruang lingkup yang diteliti adalah :

a. Aplikasi enkripsi dan dekripsi menggunakan algoritma Rijndael.

b. Objek yang dienkripsi maupun didekripsi berupa file dokumen-dokumen seperti pdf, doc, tetx, Kode ASCII, dan berkas dokumen lainnya.

c. Ekspansi Kunci yang di gunakan hanya 128 bit.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah untuk membuat sebuah aplikasi yang berfungsi untuk:

1. Memberikan keamanan untuk pengiriman data dengan metode enkripsi.
2. Penelitian ini bertujuan untuk merancang dan membuat aplikasi kriptografi enkripsi dan dekripsi menggunakan metode rijndael.
3. Dengan Aplikasi ini dokumen yang sudah dienkripsi sulit lagi dibuka dengan aplikasi tanpa dekripsike bentuk aslinya.