BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kebutuhan akan keamanan menjadi syarat utama dalam segala perihal kehidupan dijaman teknologi yang serba modern saat ini. Khususnya pengamanan data yang berisikan informasi penting tentang kerahasiaan pribadi maupun perusahaan atau organisasi tertentu dalamberbagai bidang. Untuk itu, perkembangan teknologi yang sangat pesat mendorong adanya penelitian yang nantinya dapat mensupport kebutuhan keamanan akan sebuah data.

Keamanan tidak hanya dibutuhkan oleh lembaga militer dan pemerintah, tetapi juga dibutuhkan pada sektor bisnis dan perseorangan.Hampit semua informasibiasanya bersifar rahasia dan tidak ingin diketahui oleh orang lain, terutama oleh pihak yang bertentangan denganpihak yang bertukar informasi tersebut atau yang secara sengaja maupun tidak di sengaja dapatmemanfaatkan informasi tersebut. Jika keamananpertukaran informasi ini tidak dapat dijaga, pihak-pihaklain tersebut dapat memanfaatkan informasitersebut sehingga merugikan pihak yang berhakatas informasi tersebut.

Ancaman keamanan terhadap informasi tersebut dapatberupa berbagai bentuk. Bentuk ancaman tersebutdapat berupa interupsi, intersepsi, modifikasi, danfabrikasi. Ancaman interupsi dapat mengganggуketersediaan data. Data yang ada dapat dihapussehingga pihak yang membutuhkan informasi tersebuttidak dapat

menemukan datanya. Ancaman intersepsimerupakan ancaman terhadap kerahasiaan data.Informasi yang ada disadap dan dipergunakan olehpihak yang tidak berhak sehingga merugikan pemilik data yang sah. Ancaman modifikasi yang sering dilakukan adalah memanipulasi data asli mengakibatkan kesalahan dalam penerimaaninformasi sehingga informasi yang diterima tidaksesuai dengan keinginan penerima maupunpengirimnya. Ancaman fabrikasi merupakan ancamanterhadap integritas karna terdapat pihak yang tidak diotorisasi menyisipkan/memasukkan objek-objek palsu ke sistem, laludikirimkan kepada penerima seolah-olah berasal daripengirim yang sah.

Melihat perlu dan pentingnya pengamanan data yang bersifat rahasia atau private, dan seiring dengan perkembangan teknologi informasi yang sangat pesat. Dapat di lakukan dengan memanfaatkan kriptografi algoritma keamanan data, khususnya algoritma Rijndael. Alasan tersebut yang mendasari untukmengangkat skripsi dengan judul "Perancangan Dan Implementasi Aplikasi PengamananData Menggunakan Algoritma Rijndael".

1.2 Rumusan Masalah

Dari uraian latar belakang yang telah dikemukakan, makapermasalahanyang menjadi bahasan tugas akhir ini adalah bagaimana konsep kerja dan gambaran umum algoritma Rijndael (AES) dalam menjaga keamanan serta kerahasiaan isi data dengan mengenkripsi dan dekripsi data.

1.3 Batasan Masalah

Agar tidak menyimpang dari permasalahan sehingga mencapai sasaran yang diharapkan, maka pembatasanruang lingkupbahasan sebagai berikut:

1. Tugas akhir ini membahas mengenai pembuatan aplikasi enkripsi dekripsi dengan algoritmaRijndael (AES).
2. Bahasa pemrograman yang digunakan dalam perancangan dan pemembuatan aplikasi adalah Visual Basic 6.0.
3. Aplikasi hanya berjalan pada perangkat desktop PC.
4. Panjang kalimat *(plaintext)* bisa memuat lebih dari 360 kalimat, namun untuk mempermudah penyandian disarankan kurang dari itu.
5. Data jurnalistik dalam proses penyandian yang dimaksut seperti file pada Microsoft Office, berekstensi .doc, .ppt, .exe, .txt ditambah audio, dan video berkualitas sedang.
6. Penggunaan kunci yang dipakai pada proses enkripsi-dekripsi ini sebanyak 128-192 bit.

1.4 Maksud dan Tujuan Penelitian

Adapun maksud dan tujuan yang akan dicapai adalah sebagai berikut.

1. Membantu menjelaskan tentang konsep alur kerja kriptografi dengan algoritma Rijndael.

2. Mencoba memanfaatkan perhitungan kriptografi Rijndael dan di implementasikan untuk pengamanan data jurnalistik.
3. Menjaga keaslian data dari pihak yang tidak bertanggungjawab atas isi dari informasi.
4. Sebagai syarat untuk dapat menyelesaikan jenjang pendidikan Strata-1 di STMIK AMIKOM Yogyakarta.

1.5 Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian yang dilakukan adalah untuk mengetahui sejauh manakah keamanan data dapat terjaga dengan memanfaatan algoritma Rijndael (AES). Serta dengan adanya Aplikasi yang dirancang nantinya diharapkan akan memudahkan bagi siapa saja yang ingin melindungi datanya agar tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

1.6 Metode Penelitian

Pada penyusunan skripsi yang berjudul "Perancangan Dan Implementasi Aplikasi Pengamanan Data Menggunakan Algoritma Rijndael". Metode pengumpulan data untuk mendapatkan data dan informasi yang digunakan untuk membuat penelitian adalah.

a) Studi Pustaka

Studi Pustaka yaitu metode yang digunakan sebagai pengumpulan data serta informasi yang diperoleh dari berbagai buku,*e-book*, dokumen yang relevan, artikel-artikel yang berkaitan dengan penelitian dan diajadikan acuan dalam penelitian.

b) Metode Perancangan

Tahap perancangan sistem merupakan langkah awal yang digunakan untuk menggambarkan alur kerja suatu sistem serta permodelan dari program yang akan dibuat seperti pembuatan UML, dll.

c) Pembuatan Aplikasi

Prosesmenulis dan mengelola kode sumber, mencakup semua hal yang terlibat antara penciptaan perangkat lunakyang terencana dan terstruktur.

d) Pengujian Aplikasi

Ditahap pengujian ini, yang dilakukan yaitu pengecekan hasil akhir dari implementasi algoritma Rijndael pada data yang berupa file office, audio, video dalam proses enkripsi-deksripsi tersebut terproteksi dengan baik.

e) Evaluasi

Melakukan evalusai kepada aplikasi algoritma Rijndael yang dibuat, kemudian dari keseluruhan masalah yang ditemukan, akan dijadikan saran supaya dapat dikembangkan lagi menjadi lebih baik.

1.7 Sistematika Penulisan

Penyusunan sikripsi ini bertujuan untuk memberikan gambaran yang lebih jelas dan sistematis, didalamnya terbagi menjadi lima bab dan tiap bab memiliki beberapa subbab. Berikut adalah sistematika dari skripsi ini:

BAB I PENDAHULUAN

Penguraian secara singkat mengenai awal dari Penulisan berupa Latar belakang, rumusan masalah,batasan masalah, maksud dan tujuan, metode penelitian dan sistematika penulisan.

BAB IILANDASAN TEORI

Bab ini dicantumkan semua landasan teori secara singkat dansoftware yang akan digunakan dalam penyusunan dan penulisan skripsi ini.

BAB IIIANALISA DAN PERANCANGAN

Bab ini berisi uraian mengenai analisis sistem, perancangan serta pengembangan sistem, dan hasil tampilan dari sistem.

BAB IVIMPLEMENTASI DAN PEMBAHASAN

Pada bab ini menjelaskan tentang implementasi program, pengujian, analisa pengujian serta screenshot hasil kerja dan cara penggunaannya.

BAB VPENUTUP

Bagian ini merupakan akhir penulisan skripsi yang berisi kesimpulan dari pembahasan bab-bab sebelumnya dan saran-saran untuk pengembangan lebih lanjut.