BAB I

PENDAHULUAN

I.1. Latar Belakang

Pada saat ini banyak orang membutuhkan komputer untuk menyelesaikan berbagai pekerjaannya. Komputer-komputer dapat digunakan untuk memenuhi kebutuhan pribadi maupun untuk kepentingan perusahaan atau organisasi tertentu dalam berbagai bidang. Dengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi tersebut atau pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, pihak-pihak lain tersebut dapat memanfaatkan informasi tersebut sehingga merugikan pihak-pihak yang berhak atas informasi tersebut.

Ancaman keamanan terhadap informasi tersebut dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi.. Untuk pengatasi ancaman-ancaman tersebut, diperlukanlah suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan pengamanan atau kriptografi.

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak

membacanya. Kriptografi sudah dikenal sejak ribuan tahun yang lalu. Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara. Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (*National Institute of Standard and Technology*) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (*Data Encryption Standard*) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (*Advanced Encryption Standard*) atau *Rijndael*. Oleh karena itu berdasarkan uraian diatas penulis ingin membuat Skripsi kuliah ini dengan merancang dan membuat sebuah aplikasi komputer dengan judul **" Perancangan Aplikasi Pengamanan *E-Mail* Menggunakan Metode AES (*Advanced Encryption Standard*)"**.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Berdasarkan latar belakang di atas, maka masalah dapat diidentifikasikan sebagai berikut:

1. Banyaknya pihak-pihak yang melakukan ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya.

2. Terjadinya interupsi yang dapat mengganggu ketersediaan data yaitu data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya.
3. Seringnya terjadi ancaman intersepsi yaitu merupakan ancaman terhadap kerahasiaan data.

I.2.2. Perumusahan Masalah

Berdasarkan latar belakang diatas maka rumusan masalahnya adalah bagaimana merancang sebuah aplikasi untuk pengamanan *E-mail* agar keaslian pesan dapat terjaga?

I.2.3. Batasan Masalah

Sesuai dengan topik yang diangkat dalam penelitian ini, maka pembatasan masalah yang akan dibahas hanya meliputi :

1. Tipe data *email* yang dienkripsi dan dekripsi hanya *plaintext* bukan *attachment file.*
2. Membahas enkripsi dan dekripsi email menggunakan algoritma AES Rijndael saat mengirim dan menerima *email.*
3. *Mail server* menggunakan *smtp atau imap* dan *mail client* dengan *VB.NET.*
4. Menggunakan AES 128 bit.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari dirancangnya aplikasi ini adalah merancang dan membangun suatu aplikasi pengamanan e-mail menggunakan metode AES (*Advanced Encryption Standard*).

I.3.2. Manfaat

Adapun manfaat yang akan diperoleh dari aplikasi yang akan dibangun ini adalah:

1. Agar dapat terhindar dari ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi.
2. Dapat menyajiikan informasi pesan yang dijamin keaslian datanya.
3. Diharapkan dengan adanya aplikasi ini dapat menjaga dari ancaman terhadap kerahasiaan data

I.4. Metodologi Penelitian

Metode merupakan suatu cara atau teknik yang sistematik untuk mengerjakan suatu kasus. Didalam menyelesaikan Skripsi ini penulis menggunakan 2 (dua) metode studi yaitu :

1. Studi Lapangan

Merupakan metode yang dilakukan dengan mengadakan studi langsung ke lapangan untuk mengumpulkan data yaitu peninjauan langsung ke lokasi studi. Adapun teknik pengumpulan data yang dilakukan penulis adalah.

a. Pengamatan (*Observation*)

Merupakan salah satu metode pengumpulan data yang cukup efektif untuk mempelajari suatu sistem. Kegiatannya dengan melakukan pengamatan langsung terhadap kegiatan yang sedang berjalan.

b. Sampel (*Sampling*)

Mengambil contoh – contoh data yang diperlukan khususnya E-mail berbentuk *plaintext.*

2. Studi Kepustakaan (*Library Research*)

Penulis melakukan studi pustaka untuk memperoleh data yang ada hubungan dengan penulisan Skripsi dari berbagai sumber bacaan seperti: buku, internet, dan lain – lain.

I.5. Keaslian Penelitian

Sebagai bukti penelitian yang akan dibuat, maka penelitian akan dibandingkan terhadap penelitian sejenis yang pernah dilakukan. Penelitian pertama yang diangkat oleh Aminah Rizki Lubis, Maya Silvi Lidya, B.Sc.M.Sc. dan M. Andri Budiman, S.T.,M.Comp.Sc.M.E.M dari Universitas Sumatera Utara dengan judul "Perancangan Perangkat Lunak Steganografi *Audio* Mp3 Menggunakan Metode LSB" dan penelitian kedua diangkat oleh Fricles Ariwisanto Sianturi dari Unversitas STMIK Budi Darma Medan dengan judul "Perancangan Aplikasi Pengamanan Data Dengan Kriptografi *Advanced*

Encryption Standard (AES)" perbandingannya dapat dilihat pada tabel I.1 dibawah ini :

Tabel I.1 Perbandingan Sistem Lama dan Yang Akan Dirancang

No	Materi Perbandingan	Instrumen
Penelitian pertama : Perancangan Perangkat Lunak Steganografi *Audio* Mp3 Menggunakan Metode LSB		
1.	Target	Merancang perangkat lunak steganografi Audio Mp3
2.	Solusi	Solusi didapat dengan metode LSB
3.	Bahasa pemrograman	*Visual Basic* 6.0
Penelitian kedua : Perancangan Aplikasi Pengamanan Data Dengan Kriptografi Advanced Encryption Standard (AES)		
1.	Target	Merancang aplikasi pengamanan data
2.	Solusi	Solusi didapat dengan metode Advanced Encryption Standard (AES)
3.	Bahasa pemrograman	*Visual Basic* 6.0
Penelitian yang akan dibuat : Perancangan Aplikasi Pengamanan E-Mail Menggunakan Metode AES (*Advanced Encryption Standard*)		
1.	Target	Merancang aplikasi pengamanan E-Mail
2.	Solusi	Solusi didapat dengan metode Advanced Encryption Standard (AES)
3.	Bahasa pemrograman	*VB.Net*

I.6. Sistematika Penulisan

Penulisan skripsi ini disusun secara sistematika untuk memudahkan mahasiswa dalam penyusunan skripsi. Adapun sistematika penulisan skripsi ini adalah:

BAB I : PENDAHULUAN

Dalam bab ini penulis menguraikan mengenai latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian, lokasi penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Dalam bab ini mencakup uraian penyelesaian secara teoritis serta konsep baru dalam penyelesaian masalah berkenaan dengan sistem dan fokus kajian. Adapun landasan teori yang diuraikan oleh penulis adalah: penjelasan mengenai sistem, informasi, materi tentang digunakan, serta metode konseptual yang menggambarkan cara kerja dari sistem yang akan dirancang.

BAB III : ANALISIS DAN PERANCANGAN

Pada bab ini berisi analisa sistem yang sedang berjalan, perancangan proses dalam bentuk diagram UML yang mencakup analisa dan perancangan sistem pengolahan data yang mencakup seluruh aktivitas yang terjadi pada sistem yang akan dibangun.

BAB IV : HASIL DAN UJI COBA

Dalam bab ini penulis menguraikan tentang tampilan hasil sistem yang dirancang beserta pembahasannya, kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini penulis menguraikan tentang kesimpulan dan saran untuk meningkatkan kualitas dari aplikasi yang sudah dirancang.