BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Salah satu hal terpenting dalam komunikasi menggunakan komputer dan jaringan komputer adalah untuk menjamin keamanan pesan, data, ataupun informasi dalam proses pertukaran data, sehingga menjadi salah satu pendorong munculnya teknologi Kriptografi. Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek keamanan informasi, yaitu *secrecy* (perlindungan terhadap kerahasiaan data informasi) dan *authenticity* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan.

Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. Kriptografi menggunakan berbagai macam teknik dalam upaya untuk mengamankan data. Pengiriman data dan penyimpanan data melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut. Data tersebut harus tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan di tujuan. Untuk memenuhi hal tersebut, dilakukan proses penyandian (enkripsi dan dekripsi) terhadap data yang akan dikirimkan.

Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia, sedangkan dekripsi dilakukan pada saat penerimaan dengan

cara mengubah data rahasia menjadi data asli. Jadi data yang dikirimkan selama proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

Enkripsi dapat diartikan sebagai kode atau *cipher*. Sebuah *system* pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk kata dari informasi atau yang merupakan bagian dari pesan, data, atau informasi yang di kirim. Sebuah *cipher* menggunakan suatu algoritma yang dapat meng-kodekan semua aliran data (*stream*) bit dari suatu pesan asli (*plaintext*) menjadi *cryptogram* yang tidak di mengerti. Karena *system cipher* merupakan suatu sistem yang telah siap untuk di outomasi, maka teknik ini digunakan dalam sistem keamanan jaringan komputer.

Dalam skripsi ini penulis mengambil judul : "Pembuatan Aplikasi Kriptosistem Menggunakan Metode Algoritma Vigenere Cipher".

1.2 Rumusan Masalah

Berdasarkan dari uraian latar belakang di atas, maka dapat dirumuskan beberapa masalah dalam pembuatan aplikasi ini diantaranya sebagai berikut :

1. Bagaimana merancang aplikasi kriptosistem ini menggunakan metode algoritma Vigenere Cipher.
2. Bagaimana memanfaatkan kriptosistem ini untuk dapat digunakan sebagai media mengamankan data.

1.3 Batasan

Supaya tidak keluar dari masalah yang disebutkan sebelumnya maka penulis membuat batasan rancangan yaitu:

1. Menggunakan algoritma vigenere cipher yang melakukan substitusi cipher abjad majemuk (*polyalphabetic substitution*).
2. Diimplementasikan ke dalam bahasa pemrograman visual basic 6.0 dan dijalankan di sistem operasi Windows.
3. Rancangan algoritma kriptosistem ini hanya dapat mengenkripsi dan mendekripsi data yang berupa teks atau tulisan, bukan suara maupun gambar.

1.4 Tujuan dan Manfaat

Beberapa tujuan penulisan skripsi ini adalah :

1. Untuk memenuhi syarat kelulusan untuk mendapatkan gelar kesarjanaan komputer pada jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
2. Belajar menerapkan teori-teori yang telah didapat selama di bangku kuliah dan membandingkan dengan kenyataan di lingkungan.
3. Mengimplementasikan pesan yang terenkripsi sehingga menjadi lebih aman.

Adapun manfaat yang ingin dicapai dalam pelaksanaan penelitian ini adalah :

1. Mengamalkan ilmu yang telah didapatkan dan diperoleh di STMIK AMIKOM Yogyakarta.

2. Dapat menambah ilmu pengetahuan yang telah diperoleh dan menambah wawasan baru dalam pemrograman.
3. Mengamankan data.

1.5 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan penulis antara lain :

1. Observasi

   Melakukan penganalisisan terhadap objek atau bahan yang diteliti, pengamatan ini dilakukan bersama dengan pencarian data yang dibutuhkan.

2. Studi Pustaka

   Penulis membaca literatur atau buku-buku yang berkaitan dengan permasalahan yang akan diteliti.

1.6 Sistematika Penulisan

Untuk mempermudah pemahaman dari skripsi maka dibuat sistematika yang akan disajikan dengan uraian sebagai berikut :

- **BAB I Pendahuluan,** memaparkan latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, Metode pengumpulan data dan sistematika penelitian.
- **BAB II Landasan Teori,** menjelaskan tentang tinjauan pustaka dan teori-teori yang mendasari pembuatan skripsi.
- **BAB III Analisis dan Perancangan Sistem,** bab ini akan membahas skema dan alur sistem yang akan digunakan serta konfigurasi yang digunakan.

- **BAB IV Implementasi dan Pembahasan**, bab ini akan mambahas tentang hasil dari penelitian yang dilakukan.
- **BAB V Penutup**, bab ini berisi kesimpulan dan saran.