BAB I
PENDAHULUAN

Bab ini akan menjelaskan mengenai latar belakang, perumusan masalah, tujuan, pembatasan masalah, serta sistematika penulisan laporan tugas akhir.

1.1 Latar Belakang

Keamanan data adalah suatu hal yang sangat penting pada masa sekarang ini, terutama pada masalah pengiriman data informasi tersebut. Bila suatu informasi yang seharusnya rahasia menjadi bocor, maka hal tersebut akan menyebabkan kerugian bagi pihak pengirim dan penerima informasi yang sah . Salah satu media untuk mengirimkan data informasi tersebut adalah internet, sehingga sangatlah penting dibutuhkannya proteksi informasi untuk memastikan kerahasiaan (*confidentiality*), keutuhan (*integrity*), keabsahan (*authenticity*), dan keaslian (*originality*) dari informasi tersebut.

Banyak hal yang dapat dilakukan untuk memastikan keamanan dari informasi yang dikirimkan, salah satunya dengan mengkodekan informasi tersebut menjadi data yang tidak bisa dibaca atau dimengerti oleh pihak lain, tetapi bisa dibaca oleh pihak pengirim dan penerima. Kriptografi adalah metoda yang mempelajari proteksi data dengan cara mengkodekannya. Metoda proteksi ini menggunakan berbagai teknik metoda matematis untuk mengkodekannya. Kriptografi bisa dibagi menjadi 2 model yaitu model pengkodean simetri dan model pengkodean publik (asimetri). Pengkodean simetri dibagi 2 yaitu pengkodean blok dan pengkodean *stream*. Masing-masing model pengkodean mempunyai algoritma pengkodean lebih dari satu. Penggunaan pengkodean simetris maupun publik mempunyai kelemahan dan keunggulan masing-masing. Pemakaiannya tergantung dari situasinya.

VMPC adalah salah satu dari sekian banyak algoritma pengkodean, algoritma ini ditemukan oleh Baltosz Zoltak yang berasal dari Polandia. Ia membuat aplikasi dari algoritma ini yang telah dipasarkan kepada masyarakat umum, salah satunya melalui internet. Pada situsnya diberikan algoritma dasar

dari kriptografi VMPC tersebut agar masyarakat umum yang bergerak dalam bidang keamanan informasi dapat mengkaji, dan mengujinya. Dari algoritma dasar inilah dibuat suatu aplikasi pengamanan data yang diharapkan dapat dipakai untuk mengatasi masalah-masalah pengiriman data.

1.2 Identifikasi Masalah

1. Bagaimana algoritma kunci simetri dengan metoda VMPC dapat dijadikan suatu pengaman data ?
2. Bagaimana realisasi *software* menggunakan metoda VMPC ?

1.3 Tujuan

Merealisasikan suatu *software* dengan teknik enkripsi VMPC.

1.4 Pembatasan Masalah

Menggunakan bahasa pemprograman Visual Basic untuk membuat program enkripsi dan dekripsi dengan algoritma VMPC. Tidak membahas mengenai transmisi data. Data masukan berupa teks dan file teks (*.txt).

1.5 Sistematika Pembahasan

BAB I PENDAHULUAN

Menjelaskan mengenai latar belakang pembuatan tugas akhir, identifikasi masalah, tujuan, pembatasan masalah dan sistematika pembahasan.

BAB II TEORI PENUNJANG

Menjelaskan kriptografi secara umum serta algoritma-algoritma yang menunjang pembuatan tugas akhir seperti algoritma simetrik, algoritma kunci publik, algoritma *euclidean*

BAB III IMPLEMENTASI DAN REALISASI PERANGKAT LUNAK

Dalam bab ini akan dibahas algoritma enkripsi simetris VMPC dan realisasi perangkat lunak (*software*) berdasarkan algoritma tersebut.

BAB IV HASIL PENGAMATAN

Membahas hasil pengamatan yang diperoleh berdasarkan implementasi dan realisasi perangkat lunak dari metode enkripsi simetris VMPC.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang diperoleh dari hasil pengamatan dan saran-saran yang diajukan untuk pengembangan lebih lanjut.