BAB I
PENDAHULUAN

Pada bab ini akan dijelaskan mengenai latar belakang, perumusan masalah, tujuan, pembatasan masalah, serta sistematika penulisan laporan tugas akhir.

1.1 Latar Belakang

Pada era komunikasi sekarang ini keamanan data sangatlah diperlukan untuk menjamin keutuhan nilai informasi yang dipertukarkan. Suatu informasi akan berkurang nilai informasinya atau hilang nilainya apabila dalam pengirimannya disadap atau dibajak oleh pihak yang tidak dikehendaki. Internet sebagai salah satu media pertukaran informasi sangat rawan dalam mempertahankan nilai suatu informasi, sehingga sangatlah penting dibutuhkannya proteksi informasi untuk memastikan kerahasiaan (*confidentiality*), keutuhan (*integrity*), keabsahan (*authenticity*), dan keaslian (*originality*) informasi tersebut.

Salah satu cara untuk mengatasi masalah ini ialah dengan mengkodekan informasi (data) 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.

Dari sekian banyak algoritma pengkodean, salah satunya yaitu algoritma RC2 alogaritma ini merupakan salah satu generasi awal sebelum alogaritma RC4 maupun RC6, alogaritma ini bersifat simentris artinya kunci untuk mengenkripsi sama dengan kunci untuk mendekripsi alogaritma RC2 ini muncul karena saat itu alogaritma DES yang menjadi alogaritma yang merupakan standar baku sudah

mulai banyak ditembus oleh para hacker. RC2 dirancang oleh Ron Rivest di tahun 1987. "RC" singkatan dari "Ron's Code" atau "Rivest Cipher", RC2 akan bisa ditembus dengan 2^{34} kali percobaan.

1.2 Identifikasi Masalah

1. Bagaimana algoritma kunci simetri dengan metoda RC2 dapat dijadikan suatu pengaman data ?
2. Bagaimana realisasi *software* menggunakan metoda RC2 ?

1.3 Tujuan

1. Merealisasikan suatu *software* dari suatu pengamanan data dengan teknik enkripsi RC2.

1.4 Pembatasan Masalah

Menggunakan bahasa pemprograman Borland Delphi untuk membuat program enkripsi dan dekripsi dengan algoritma RC2. 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 RC2 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 RC2

BAB V KESIMPULAN DAN SARAN

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