BAB I
PENDAHULUAN

I.1. LATAR BELAKANG

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut dikirim dan diterima oleh pihak atau orang yang berkepentingan, apakah pesan, data, atau informasi masih *authenticity*. Pesan, data, atau informasi akan tidak berguna lagi apabila di tengah jalan informasi itu disadap atau dibajak oleh orang yang tidak berhak atau berkepentingan.

Keamanan dan kerahasian data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital, seperti sistem pertahanan, sistem perbankan, sistem bandara udara dan sistem-sistem yang lain setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih di sebabkan karena kemajuan bidang jaringan komputer dengan konsep *open sistem*-nya sehingga siapapun, dimanapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut. Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam suatu jaringan komputer maka di perlukan beberapa enkripsi guna membuat pesan, data, atau informasi agar tidak dapat dibaca atau dimengerti oleh sembarang orang, kecuali untuk penerima yang berhak.

Ada banyak model dan metode enkripsi, salah satu di antaranya adalah enkripsi dengan algoritma *Software Encryption Algorithm* (SEAL). Model ini merupakan salah satu algoritma kunci simetris yang berbentuk *stream chipper*.

Algoritma ini ditemukan pada tahun 1993 oleh Rogaway dan Coppersmith. SEAL menggunakan panjang kunci dari 160 bit yang digunakan untuk menginisialisasikan tabel. Tabel ini digunakan untuk generasi yang berikut dari *pseudo random* yang menggunakan XOR dengan *plaintext* untuk menghasilkan *chipertext*.

I.2. IDENTIFIKASI MASALAH

Bagaimana cara memetakan suatu *plaintext* (pesan) menjadi *ciphertext* (pesan yang telah terenkripsi) dengan menggunakan enkripsi SEAL dan memetakan *ciphertext* menjadi *plaintext*?

I.3 MAKSUD DAN TUJUAN

Untuk melindungi pesan, data, atau informasi agar tidak dapat dibaca oleh orang-orang yang tidak berhak maka diperlukan enkripsi yang dapat mengacak pesan tersebut agar tidak dapat dibaca oleh orang lain. Dalam hal ini enkripsi yang digunakan adalah Stream Cipher dengan metoda SEAL.

I.4 PEMBATASAN MASALAH

Pada tugas akhir ini masalah yang dihadapi akan disederhanakan agar lebih mudah dipahami, maka masalah yang akan dibahas dalam tuga akhir ini dibatasi pada:

- Bahasa pemograman yang digunakan yaitu Visual Basic 6.0

I.5. SISTEMATIKA PEMBAHASAN

Laporan tugas akhir ini disusun dalam lima bab. Masing-masing bab berisi pokok bahasan yang berhubungan dengan enkripsi dan dekripsi dengan metoda SEAL.

Bab I Pendahuluan

Dalam bab ini, akan dipaparkan gambaran permasalahan dan tujuan tugas akhir ini. Bab ini diawali dengan latar belakang permasalahan, identifikasi masalah, maksud dan tujuan, pembatasan masalah, dan yang terakhir adalah sistematika pembahasan laporan.

Bab II Teori-Teori Penunjang

Bab ini memuat teori-teori dasar mengenai enkripsi dan dekripsi, basic XOR, macam-macam kunci, stream cipher, SEAL dan teori dasar Visual Basic.

Bab III Perancangan dan Realisasi

Pada bab ini akan dibahas perancangan pembuatan program enkripsi dan dekripsi stream cipher dengan metoda SEAL. Pada akhir bab ini akan digambarkan pula *flowchart* pemrograman cara kerja pemograman SEAL.

Bab IV Pengujian dan Data Pengamatan

Dalam bab ini akan dipaparkan hasil pengujian yang telah dilakukan terhadap program SEAL.

Bab V Kesimpulan dan Saran

Berisi kesimpulan-kesimpulan yang diambil berdasarkan hasil pengujian berupa data pengamatan dan saran-saran untuk pengembangan lebih lanjut.