BAB I
PENDAHULUAN

1.1 Latar Belakang

Informasi menentukan hampir setiap elemen dari kehidupan manusia. Informasi sangat penting artinya bagi kehudupan karena tanpa informasi maka hampir semuanya tidak dapat dilakukan dengan baik.

Pada zaman teknologi informasi, suatu pesan atau informasi merupakan suatu aset yang sangat berharga dan harus dilindungi. Kemajuan teknologi komputer membantu semua aspek kehidupan manusia. Dari hal yang sederhana sampai yang sangat rumit sekalipun bisa dikerjakan komputer. Contoh dari kemajuan teknologi komputer yang paling nyata yang dapat digunakan oleh semua orang adalah kecepatan dalam menyampaikan pesan dari tempat yang jauh. E-mail (*electronic mail*) merupakan fasilitas yang ditawarkan oleh kemajuan teknologi. Rupa pesan semakin bermacam-macam, seperti teks, gambar, suara, video, ataupun tabel. Pesan pun bisa dikirim menggunakan jasa pos, kurir, jaringan elektronik (internet), dan bisa disimpan di dalam buku, *hard-disc*, SC, DVD, kaset, dan lain-lain.(Ariyus, 2008).

Dengan adanya kemajuan dalam teknologi informasi, komunikasi dan komputer maka kemudian timbul masalah baru, yaitu masalah keamanan. Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi, seperti kejahatan komputer yang mencakup pencurian, penipuan, pemerasan, kompetisi, dan banyak lainnya. Jatuhnya informasi ke pihak lain, misalnya lawan bisnis, dapat menimbulkan kerugian bagi pemilik informasi.Oleh karena itu diperlukan suatu cara untuk menyamarkan suatu pesan yang biasa disebut kriptografi. Pesan adalah data atau informasi yang dapat dimengerti maknanya atau biasa disebut *plaintext.* Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi data, dan lain-lain) atau yang disimpan di dalam media perekaman (kertas, *storage*, dan lain-lain). Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan disandikan ke bentuk lain. Bentuk pesan yang tersandi disebut *ciphertext*. *Ciphertext* harus dapat ditransformasi kembali menjadi *plaintext* (Munir, 2004).

Terdapat berbagai macam algoritma yang digunakan dalam menjaga keamanan informasi. Salah satu diantaranya adalah Algoritma CAST-128. Algoritma CAST-128 ini disebut sebagai salah satu algoritma kriptografi yang kuat terhadap berbagai macam kriptanalisis, termasuk *differential* dan *linear attack*. Oleh karena itu, tidak salah jika dikatakan bahwa CAST-128 dapat menjadi kandidat kuat untuk pemakaian enkripsi untuk keamanan komunitas internet. (Gunawan. 2006).

Algoritma ini diciptakan pada tahun 1996 oleh Carlisle Adams dan Stafford Tavares dari kanada. CAST-128 termasuk kelas algoritma enkripsi yang merupakan jaringan Feistel. Secara umum algoritma ini mirip dengan algoritma Data Encryption Standart (DES) (Ariyus, 2008). Algoritma ini memanfaatkan jaringan *feistel* 16 kali putaran, 64-bit blok teks-asli dibagi menjadi dua bagian yang sama yaitu bagian kiri dan bagian kanan dengan panjang yang sama dengan panjang 32bit, 8x32 entri *S-Box* dan masukan sebuah kunci dengan panjang sampai 128-bit(Ariyus, 2008).

Dalam penelitian ini akan dibahas dibahas waktu proses dan ketahanan algoritma *CAST-128*. Waktu proses dari algoritma *CAST-128* ini akan terdiri dari waktu proses pembangkitan kunci, waktu untuk enkripsi dan dekripsi *file*. Untuk ketahanan algoritma, metode yang sering dipakai adalah *avalanche effect*. Dimana suatu algoritma akan dikatakan baik dalam hal ketahanan terhadap serangan jika nilai *avalanche effect*-nya berkisar antara 45-60% (Rudianto, 2004). Dengan latar belakang tersebut maka dilakukan penelitian untuk skripsi ini dengan judul "**IMPLEMENTASI ALGORITMA KRIPTOGRAFI CAST-128 TERHADAP TEKS".**

1.2 Rumusan Masalah

Rumusan masalah yang akan dijadikan obyek penelitian yaitu :

1. Bagaimana implementasi algoritma *CAST-128* untuk melakukan enkripsi dan dekripsi *file* teks.
2. Berapa waktu proses algoritma.
3. Berapa nilai ketahanan algoritma dengan menggunakan metode *avalanche effect.*

1.3 Tujuan penelitian

1. Implementasi enkripsi dan dekripsi *file* teks menggunakan algoritma *CAST-128*.
2. Menghitung waktu proses algoritma *CAST-128*.
3. Menghitung nilai *avalanche effect* algoritma *CAST-128* untuk mengetahui ketahanan terhadap serangan.

1.4 Manfaat

Manfaat yang ingin dicapai dari penulisan skripsi ini adalah sistem yang memiliki ketahanan terhadap serangan kriptanalisis yang mampu membantu menyelesaikan masalah keamanan data informasi.

1.5 Batasan Masalah

Pada penelitian ini akan diberi batasan - batasan masalah sebagai berikut :

1. Perangkat lunak akan berupa aplikasi *web*.
2. Uji coba waktu proses enkripsi dan dekripsi akan dilakukan sebanyak lima kali dengan *file* teks **.txt*.
3. Data yang digunakan dalam uji coba waktu proses adalah *file* teks dengan ukuran beragam mulai dari 50KB hingga 500KB.
4. Data yang digunakan dalam uji *avalanche effect* adalah *file* teks dan *file* hasil enkripsi dengan ukuran beragam mulai dari 8*bytes* sampai 40*bytes*.
5. Jenis uji coba *avalanche effect* terdiri dari 3 macam yaitu : uji coba pada *plaintext,* pada *chipertext* dan pada *Key*.
6. Uji coba *avalanche effect* dilakukan pada skala bit dan *byte*. Dengan jumlah bit atau *byte* sebanyak satu dan dua.
7. Posisi perubahan pada saat uji coba *avalanche effect* dibagi menjadi 3 bagian yaitu : posisi bit/*byte* awal, tengah dan akhir.

1.6 Sistematika Penulisan

Buku tugas akhir ini terdiri dari beberapa bab, yang dijelaskan sebagai berikut:

1. **BAB I. PENDAHULUAN**
   Bab ini berisi latar belakang masalah, tujuan dan manfaat pembuatan tugas akhir, permasalahan, batasan masalah, dan sistematika penyusunan tugas akhir.
2. **BAB II. TINJAUAN PUSTAKA**
   Bab ini membahas beberapa teori penunjang yang berhubungan dengan pokok pembahasan dan mendasari pembuatan tugas akhir ini.
3. **BAB III. METODOLOGI DAN PERANCANGAN SISTEM**
   Bab ini membahas desain dari sistem yang akan dibuat meliputi : arsitektur, proses dan antarmuka perangkat lunak.
4. **BAB IV. IMPLEMENTASI DAN PEMBAHASAN**
   Bab ini membahas implementasi dari desain sistem disertai dengan potongan *source code* yang penting dalam aplikasi dan membahas uji coba dari aplikasi yang dibuat dengan melihat *output* yang dihasilkan oleh aplikasi, dan evaluasi untuk mengetahui kemampuan aplikasi.
5. **BAB V. PENUTUP**
   Bab ini berisi kesimpulan dari hasil uji coba yang dilakukan serta saran untuk pengembangan aplikasi selanjutnya.