1. Pendahuluan

1.1 Latar Belakang

Perkembangan suatu organisasi, perusahaan, maupun negara ditentukan oleh informasi, karena hal itu merupakan suatu hal yang sangat penting. Informasi tersebut mengalami pertukaran seperti contohnya semakin mudah para pelaku kejahatan memanfaatkannya dengan memasuki maupun memanipulasi informasi. Oleh karena itu dibutuhkan sebuah keamanan pada sistem informasi untuk menanggulanginya.

Banyak hal yang dapat dilakukan untuk menanggulangi masalah keamanan informasi tersebut, salah satunya adalah dengan kriptografi. Tanpa kita sadari, kehidupan kita sudah dikelilingi oleh kriptografi, antara lain transaksi di mesin ATM, kartu kredit, mengakses internet, pembicaraan melalui telepon genggam. Sehingga kita sulit untuk memisahkan diri dari kriptografi.

Dalam kriptografi mempunyai banyak algoritma untuk menyelesaikan setiap permasalahan. Akan tetapi setiap algoritma mempunyai prinsip yang sama yaitu mengubah data jelas (*plainteks*) menjadi data sandi (*ciphertext*). Plaintext akan dikirimkan melalui saluran telekomunikasi maupun media lain. Agar data tersebut tidak dapat dimengerti oleh pihak lain, plainteks akan diubah (disandikan) dalam bentuk lain yang tidak dapat dimengerti oleh orang lain. Penyandian plainteks menjadi cipherteks biasa dinamakan *enkripsi*. Sedangkan untuk dapat membaca kembali sebuah cipherteks maka harus ditransformasikan kembali sehingga menjadi plainteks semula. Transformasi itu dinamakan *dekripsi*.

Contoh algoritma kriptografi adalah algoritma Gost dan algoritma Serpent yang mempunyai kelebihan dan kekurangan masing-masing. Algoritma Gost, *Gosudarstvenny Standart*, dikembangkan pada tahun 1970 oleh pemerintah Soviet untuk penyandian pemerintahan. Gost dibangun menggunakan jaringan Feistel dengan mempunyai panjang kunci 256 bit, beroperasi pada blok pesan dengan panjang 64-bit dan 32 putaran dengan masing putaran mempunyai 8 kunci internal. Belum adanya publikasi mengenai kripanalisis dari algoritma Gost ini memperlihatkan ketahanan algortima ini yang baik. Algoritma Serpent dipublikasikan pada tahun 1998 pada perlombaan enkripsi AES dan menduduki peringkat kedua. Serpent beroperasi dengan 128-bit dan panjang kunci 128, 192, dan 256 bit dengan 32 putaran yang mempunyai 32 kunci internal. Serpent dirancang untuk menyediakan cipher yang aman dan tahan terhadap semua jenis serangan cipher.

Tugas Akhir ini akan dibuat sebuah perangkat lunak yang dapat membandingkan algoritma Gost dan Serpent. Kedua algoritma ini mempunyai perbedaan tahun yang cukup jauh, akan tetapi keduanya mempunyai ketahanan yang mendekati, dan mempunyai putaran kunci yang sama. Tugas akhir ini akan menganalisa dengan menggunakan parameter waktu proses, *avalance effect*, dan tingkat keamanan, yang dibutuhkan untuk melakukan enkripsi dan dekripsi dari algoritma Gost dan Serpent.

1.2 Perumusan masalah

Perumusan masalah dalam Tugas Akhir ini adalah sebagai berikut :

1. Bagaimana membangun suatu perangkat lunak menggunakan algoritma Gost dan Serpent.
2. Bagaimana menganalisa perbandingan algoritma kriptografi Gost dan Serpent dengan parameter waktu proses, *avalance effect*, dan tingkat keamanan yang dibutuhkan untuk enkripsi dan dekripsi.

Ruang lingkup yang menjadi batasan Tugas Akhir ini adalah:

1. Perangkat lunak akan menghitung waktu proses untuk enkripsi dan dekripsi serta *avalance effect* pada algoritma Gost dan Serpent.
2. Parameter tingkat keamanan diselesaikan dengan uji statistik.
3. Mode Operasi yang digunakan adalah *Electronic Code Book* (ECB).
4. Ukuran kunci yang digunakan adalah 256 bit.

1.3 Tujuan Penulisan

Adapun Tujuan dari Tugas Akhir ini ialah :

1. Membangun perangkat lunak dengan menggunakan algoritma Gost dan Serpent
2. Menghitung waktu proses untuk enkripsi dan dekripsi serta *avalance effect* dari algoritma Gost dan Serpent.
3. Menganalisa kekurangan dan kelebihan dari algoritma Gost dan Serpent dengan membandingkan parameter waktu proses, *avalance effect*, dan tingkat keamanan.

1.4 Metodologi penyelesaian masalah

Metodologi yang digunakan dalam menyelesaikan Tugas Akhir ini adalah :

1. Studi Literatur dan pustaka yang bertujuan untuk mempelajari dan memahami algoritma Gost dan Serpent serta materi lain yang mendukung Tugas Akhir ini, antara lain :
   a. Pemahaman tentang sejarah dan prinsip-prinsip dasar kriptografi.
   b. Literatur mengenai prinsip dasar, *source code*, implementasi dan hal-hal lain yang berhubungan dengan algoritma Gost dan Serpent.
   c. Literatur-literatur lain yang mendukung Tugas Akhir ini.
2. Melakukan analisis terhadap materi yang didapat, antara lain :
   a. Mencari perbedaan antara algoritma Gost dan Serpent untuk dilakukan perbandingan (sebagai permasalahan dalam Tugas Akhir ini, yaitu mengenai waktu yang dibutuhkan, *avalance effect*, dan tingkat keamanan).
   b. Menganalisis kebutuhan dan spesifikasi yang dibutuhkan dalam membangun perangkat lunak.
3. Merancang perangkat lunak yang didapat dari hasil analisis sebelumnya, antara lain :
   a. Perancangan perangkat lunak dengan menggunakan Data Aliran Diagram, spesifikasi proses, dan kamus data.

4. Membangun perangkat lunak dengan menggunakan Borland Delphi 7 untuk algoritma Gost dan Serpent.
5. Melakukan pengujian dan menganalisis perangkat lunak yang telah dibangun berdasarkan waktu yang dibutuhkan untuk enkripsi dan dekripsi data dan *avalance effect*
6. Membuat laporan Tugas Akhir dan kesimpulan.

1.5 Sistematika Penulisan

Tugas Akhir ini disusun dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini menjelaskan latar belakang penelitian, perumusan masalah yang dibahas serta ruang lingkup yang menjadi batasan masalah, tujuan yang ingin dicapai, metode penyelesaian masalah, dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini membahas teori yang mendukung penyusunan Tugas Akhir ini, yaitu : pengenalan sistem kriptografi, algoritma kriptografi, mode operasi, dasar matematis, pengenalan algoritma Gost dan Serpent.

BAB III ANALISA DAN PERANCANGAN SISTEM

Bab ini menjelaskan hasil analisis dari kebutuhan sistem dan perancangan algoritma Gost dan Serpent dengan menggunakan Data Aliran Diagram.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini menjelaskan hasil implementasi dan pengujian perangkat lunak dari perbandingan algoritma Gost dan Serpent.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil penelitian Tugas Akhir ini serta saran-saran untuk pengembangan lebih lanjut.