BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada umumnya, perancangan suatu algoritma enkripsi harus dapat memenuhi kebutuhan pengguna yaitu memiliki karakteristik cepat, kuat, sederhana dan tidak terhalang lisensi. Blowfish merupakan salah satu algoritma yang diciptakan oleh Bruce Schneier pada tahun 1993, perancangannya dimaksud untuk menggantikan *Data Encryption Standard* (DES) dan dapat memenuhi karakteristik di atas. Blowfish kemudian dapat menarik perhatian publik dan dianggap sebagai algoritma terbaik karena telah digunakan dalam dunia open source sebagai *Open Cryptography Interface* (OCI) pada kernel Linux versi 2.5 ke atas.

Seiring berkembangnya algoritma enkripsi kesuksesan Blowfish mulai memudar, karena pada saat pengimplementasiannya Blowfish tidak cocok untuk aplikasi yang sering memerlukan perubahan kunci. Sehingga Bruce Schneier melakukan pengembangan algoritma Blowfish menjadi algoritma Twofish dan berhasil masuk menjadi lima kandidat algoritma standar enkripsi *Advanced Encryption Standard* (AES). Tujuan perancangan Twofish sendiri agar dapat digunakan secara efisien baik pada software maupun hardware, rancangan yang sederhana dan mudah diimplementasikan. Twofish juga diharapkan dapat memenuhi kebutuhan pengguna dalam aplikasi enkripsi, serta memiliki kelebihan performansi dari algoritma Blowfish.

Algoritma Blowfish dan Twofish merupakan algoritma enkripsi yang kuat dan masih banyak digunakan dalam aplikasi enkripsi, namun dalam pengimplementasiannya harus disesuaikan dengan kebutuhan pengguna. Alasan pemilihan kedua algoritma di atas karena algoritma Blowfish dan Twofish memiliki hubungan yang sangat erat diantaranya Twofish merupakan perkembangan dari Blowfish, keduanya sama-sama tergolong jenis algoritma cipher blok, dirancang oleh orang yang sama (Bruce Schneier) dan dalam proses enkripsinya kedua algoritma tersebut menggunakan jaringan feistel.

Secara umum, Twofish dirancang agar lebih baik dan lebih unggul daripada Blowfish, namun sebaik dan seunggul apakah Twofish dibandingkan dengan Blowfish dari sisi perbedaan performansi yang akan dianalisis. Dengan adanya permasalahan di atas, maka pada Tugas Akhir ini akan dilakukan penelitian yang bertujuan untuk menentukan kelebihan dan kekurangan algoritma Blowfish dan Twofish berdasarkan kebutuhan pengguna. Penelitian akan dilakukan berdasarkan perbandingan performansi yang dihasilkan kedua algoritma. Implementasi Tugas Akhir ini akan menggunakan Visual Basic 6.0 sebagai media perbandingan performansi enkripsi dan dekripsi data.

1.2 Perumusan Masalah

Blowfish dan Twofish merupakan algoritma kripografi kunci simetri dan juga merupakan cipher blok. Permasalahan yang dijadikan objek penelitian dan pengembangan tugas akhir ini adalah:

1. Bagaimana mekanisme kerja enkripsi dan dekripsi data dengan menggunakan algoritma Blowfish dan Twofish.
2. Bagaimana perbandingan performansi algoritma Blowfish dan Twofish berdasarkan parameter waktu proses enkripsi dan dekripsi, perbandingan besar file input / output enkripsi dan dekripsi, nilai *avalanche effect* enkripsi dan dekripsi.

1.3 Tujuan Penulisan

Tujuan penulisan dari Tugas Akhir ini sebagai berikut :

1. Menghasilkan suatu perangkat lunak yang dapat menghasilkan perbandingan performansi antara algoritma Blowfish dan Twofish, sehingga dapat dilihat performansi masing-masing algoritma berdasarkan parameter perbandingan yang dianalisa.
2. Menganalisis perbandingan performansi (waktu proses enkripsi/dekripsi, perbedaan besar file input/output, nilai *avalanche effect*) algoritma Blowfish dan Twofish.

1.4 Batasan Masalah

Batasan masalah dalam membandingkan algoritma Blowfish dan Twofish pada tugas akhir ini adalah :

1. File inputan yang digunakan adalah file teks atau tulisan.
2. Parameter ukuran yang dianalisa adalah :
    a. Waktu proses enkripsi dan dekripsi.
    b. Perbedaan besar file input dan output.
    c. Nilai *Avalanche Effect*.

1.5 Metodologi Penulisan

Metodologi yang digunakan untuk menyelesaikan masalah dalam Tugas Akhir ini adalah

1. Studi Literatur
   Studi literatur dari beberapa buku, jurnal, artikel yang membahas tentang tipe file teks, kriptografi, algoritma cipher blok, kunci simetri, blowfish, twofish dan karakteristik serta pembuatan aplikasi.
2. Analisis dan Desain
   Tahap ini meliputi analisis kebutuhan serta penyelesaian masalah untuk merancang perangkat lunak enkripsi dan dekripsi file teks dengan menggunakan

algoritma Blowfish dan Twofish. Desain perangkat lunak yang akan dibangun berdasarkan proses.

3. Perancangan dan Implementasi Sistem
   Tahap ini meliputi pembangunan perangkat lunak yang telah dirancang pada tahap sebelumnya. Pembangunan perangkat lunak menggunakan Visual Basic 6.0.
4. Analisis dan Pengujian
   Pada tahap ini adalah melakukan analisis terhadap hasil pengujian perangkat lunak dalam enkripsi pada file. Untuk mengukur waktu, besar file input/output, nilai *avalanche effect* dengan menggunakan ukuran file teks dan panjang kunci yang berbeda-beda. Sehingga didapatkan rata-rata perbedaan performansi kedua algoritma. Analisa dan perhitungan keluaran dari sistem yang telah dibangun.
5. Penyusunan Laporan
   Hasil penelitian akan disusun menjadi suatu laporan yang meliputi aspek-aspek dalam penelitian yaitu teori, perancangan dan implementasinya, serta membuat kesimpulan dan saran dari hasil penelitian

1.6 Sistem Penulisan

Struktur Pembahasan Tugas Akhir ini disusun berdasarkan Sistematika Penulisan sebagai berikut :

BAB I. Pendahuluan

Dalam pendahuluan akan dijelaskan secara singkat latar belakang, perumusan masalah, tujuan penulisan, batasan masalah, metoda penelitian dan sistematika penulisan.

BAB II. Landasan Teori

Pada bab ini akan dijelaskan tentang algoritma kunci simetri, teori dan implementasi sistem, penjelasan algoritma Blowfish dan Twofish, konsep dasar kedua algoritma serta metode enkripsi cipher blok, metode perhitungan waktu, besar file, *avalanche effect.*

BAB III. Analisis Desain dan Perancangan Sistem

Bab ini berisi analisis terhadap seluruh masalah seperti kebutuhan perangkat lunak, dan membahas mengenai perancangan perangkat lunak sistem

BAB IV. Implementasi dan Analisis Hasil Pengujian

Bab ini berisi implementasi dari sistem yang dibuat, dan melakukan analisa hasil pengujian aplikasi yang dibuat berdasarkan waktu, besar file input/output, *avalanche effect*.

BAB V. Kesimpulan dan Saran

Pada bab akhir terdapat kesimpulan dari seluruh rangkaian penelitian yang dilakukan dan saran untuk pengembangan selanjutnya.