BAB 1
PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Di mana kebenaran dan keaslian suatu informasi sangat penting baik pada saat pengiriman ataupun pada saati nformasi tersebut diterima. Pesan, data, atau informasi tidak akan berguna lagi apabila pada saat pengiriman informasi tersebut disadap atau dibajak oleh orang yang tidak berhak atau berkepentingan.

Saat ini sistem komputer yang terpasang dengan jaringan *LAN* makin mudah diakses. Sistem *sharing* data dan akses jarak jauh menyebabkan masalah keamanan menjadi salah satu kelemahan komunikasi data seperti jaringan *LAN*. Disamping itu kecenderungan lain saat ini adalah memberikan tanggung jawab sepenuhnya ke komputer untuk mengelola aktifitas pribadi dan bisnis seperti *transfer* data antar computer dengan jaringan *LAN*. Untuk itu diperlukan sistem komputer yang memiliki tingkat keamanan yang dapat terjamin.

Berdasarkan kenyataan tersebut, perlu ada suatu pengamanan informasi pada saat pengiriman informasi. Untuk melakukan ini ada suatu cara yang biasa disebut penyandian data. Dalam penelitian ini akan mencoba mengimplementasikan suatu cabang ilmu matematika yang disebut dengan kriptografi. Dengan adanya sebuah kriptografi yang meliputi proses enkripsi dan dekripsi maka pesan, data, maupun informasi dapat dikodekan sehingga orang yang tidak berkepentingan tidak dapat membaca informasi tersebut serta

mengembalikannya kembali seperti semula, selain orang yang mengetahui kunci *(Key)*untuk mendeskripsikannya.

Dengan adanya dua algoritma kriptografi yang akan dipakai dalam mengamankan data. Di mana kedua algoritma tersebut termasuk dalam kategori kunci *chipper blok* yang banyak digunakan pada saat ini. Kedua algoritma ini beroperasi pada blok bit dan kedua algoritma ini banyak digunakan karena merupakan algoritma kunci simetri yang kuat terhadap serangan (*attack*). Dengan bertitik tolak pada masalah tersebut maka akan dicoba untuk membandingkan dua algoritma kriptografi yaitu algoritma *Rijndael* dan algoritma *Twofish*. Dengan adanya dua dari sekian banyak algoritma kriptografi tersebut, di mana masing-masing algoritma mempunyai kelebihan dan kekurangan dalam melakukan proses enkripsi dan dekripsi data serta waktu prosesnya, maka dari itu akan dilakukan perbandingan terhadap kedua algoritma tersebut pada jaringan *Local Area Network (LAN)* di komputer untuk mengetahui algoritma mana yang paling cepat dalam proses pengamanan data teks melalui jaringan *Local Area Network (LAN)*.

1.2 Perumusan Masalah

Berdasarkan uraian latar belakang di atas, maka perumusan masalah yang akan dibahas dalam tugas akhir ini adalah sebagai berikut :

1. Bagaimana cara membangun aplikasi untuk membandingkan algoritma *Rijndael* dan algoritma *Twofish*.
2. Bagaimana langkah-langkah dalam proses enkripsi dan dekripsi pada algoritma *Rijndael* dan *Twofish.*

3. Bagaimana menganalisis kelebihan dan kekurangan dari kedua algoritma tersebut dalam proses penyandian data teks.

1.3 Maksud dan Tujuan

1.3.1 Maksud

Maksud dari penulisan tugas akhir ini adalah merancang dan membangun perangkat lunak pengamanan data dengan menggunakan dua algoritma kriptografi yaitu algoritma *Rijndael* dan algoritma *Twofish*.

1.3.2 Tujuan

Tujuan yang akan dicapai dalam pembangunan perangkat lunak adalah :

1. Untuk mengetahui perbandingan waktu pada saat proses enkripsi dan dekripsi dari kedua algoritma tersebut.
2 Untuk mengetahui perbandingan kapasitas file pada saat sebelum dan sesudah serta perbandingan waktu pengiriman data secara *streaming* pada proses enkripsi dan dekripsi dari kedua algoritma tersebut.
3 Untuk mengetahui kelebihan dan kelemahan dari masing-masing algoritma tersebut dalam proses penyandian data teks.

1.4 Batasan Masalah / Ruang Lingkup Kajian

Pembahasan permasalahan diharapkan tidak menyimpang dari pokok permasalahan, sehingga diperlukan batasan masalah.Adapun batasan dari penulisan tugas akhir ini adalah sebagai berikut :

1. Membahas hanya mengenai tentang algoritma *Rijndael* dan algoritma *Twofish* pada proses penyandian data.
2. Pada kedua algoritma ini menggunakan kunci 128-*bit*.

3. Penggunaan waktu di aplikasi untuk menganalisis proses enkripsi dan dekripsi, sehingga bisa dilihat berapa lama prosesnya.
4. Kunci pada saat mengenkripsi sama dengan kunci pada saat dekripsi (simetris).
5. Hanya dapat mengenkripsi dan mendekripsi sebuah file yang ada pada komputer.
6. Data yang akan dicoba diamankan adalah data yang ada pada komputer seperti hanya data teks dengan *extension* doc, txt, dan pdf.
7. Simulasi ini hanya dilakukan untuk membandingkan dalam hal kecepatan proses enkripsi dan dekripsi suatu data dan kapasitas file pada proses enkripsi dan dekripsi.
8. Pengujian program ini dilakukan pada sebuah jaringan LAN (*Local Area Network*), yaitu pada 2 komputer atau lebih.
9. Sistem ini dibangun dengan menggunakan *tools Visual Basic* 6.0 dan berbasis *desktop*.
10. Sistem operasi yang mendukung *software* agar dapat bekerja secara optimal adalah minimal *Windows XP SP2*.

1.5 Metodologi Penelitian

Kegiatan yang dilakukan untuk membandingkan kedua algoritma dalam hal penyandian data yaitu algoritma *Rijndael* dan algoritma *Twofish* untuk pemecahan masalah yang ada, yaitu mengetahui kekurangan dan kelebihan dari kedua algoritma tersebut. Maka dilakukan analisis terhadap kedua algoritma tersebut.

1.5.1 Metode Penelitian

Metode penelitian yang digunakan adalah metode deskiptif. Metode ini tertuju pada pemecahan masalah yang ada pada masa sekarang secara aktual, data yang dikumpulkan awalnya disusun, dijelaskan, dianalisis, dan kemudian diinterpretasikan [7].

1.5.2 Metode Pengumpulan Data

Digunakan untuk mengumpulkan data-data yang diperlukan selama proses penyusunan tugas akhir yang diawali dengan tahap perancangan sampai dengan implementasi dan pengujian.

Jenis metode yang digunakan dalam penelitian adalah sebagai berikut :

a. Studi Pustaka

   Teknik pengumpulan data dengan cara membaca dan menganalisa buku-buku serta media cetak lainnya yang ada kaitannya dengan judul penelitian.

b. Observasi

   Teknik pengumpulan data dengan mengadakan penelitian dan peninjauan langsung ke lapangan terhadap objek yang diteliti.

1.5.3 Metode Perancangan Perangkat Lunak

Metode perancangan perangkat lunak yang digunakan adalah Waterfall. Dalam metode ini terdapat empat bagian, yaitu :

a. *System Engineering*

Tahap untuk menetapkan berbagai kebutuhan dari semua elemen yang diperlukan sistem dan mengalokasikannya ke dalam pembentukan perangkat lunak.

b. *System Analysis*

Merupakan tahap menganalisis hal-hal yang diperlukan dalam pelaksanaan pembuatan perangkat lunak.

c. *System Design*

Tahap penerjemahan dari data yang dianalisis kedalam bentuk yang mudah dimengerti oleh *user*.

d. *System Coding*

Tahap penerjemahan data atau pemecahan masalah yang telah dirancang kedalam bahasa pemrograman tertentu.

e. *System Testing*

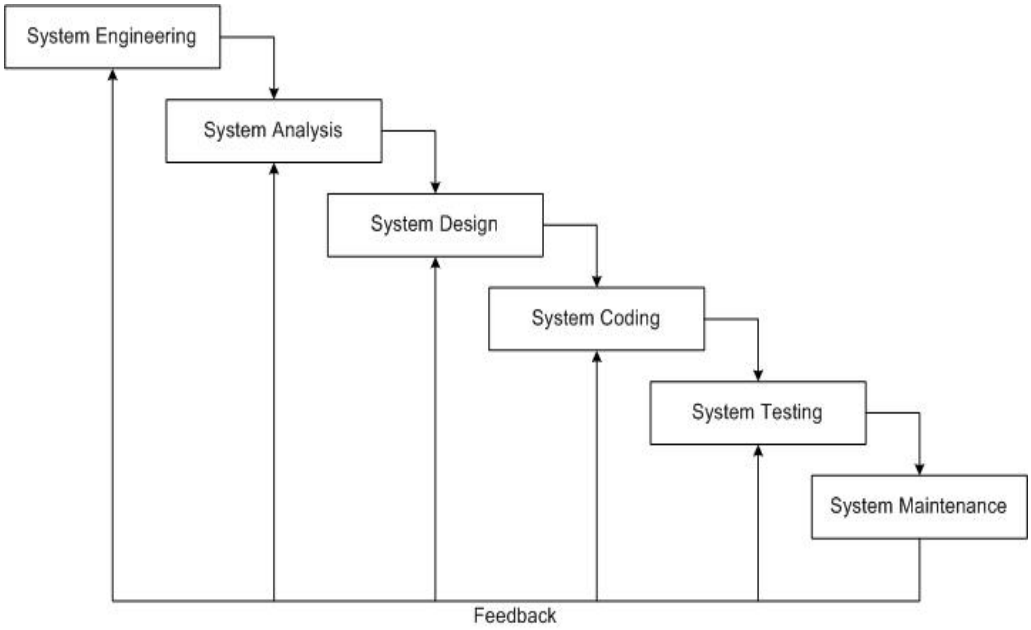
Merupakan tahap pengujian terhadap perangkat lunak yang dibangun.

f. *System Maintenance*

Tahap akhir dimana suatu perangkat lunak yang sudah selesai dapat mengalami perubahan-perubahan atau penambahan sesuai dengan permintaan pengguna.

g. *Feedback*

Merupakan respon dari pengguna sistem yang bisa digunakan untuk mengetahui sejauh mana aplikasi yang dibangun diterima oleh pengunanya.



Gambar 1.1 Metode *Waterfall* [3]

1.6 Sistematika Penulisan

Sistematika penulisan ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan Tugas Akhir ini adalah sebagai berikut :

BAB 1 PENDAHULUAN

Menguraikan tentang latar belakang permasalahan, mencoba merumuskan inti permasalahan yang dihadapi, menentukan tujuan dan kegunaan penelitian yang kemudian diikuti dengan pembatasan masalah, serta sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Membahas berbagai konsep dasar teori yang mendasari permasalahan dan didapat dari literature-literatur, referensi, dan informasi-informasi lainnya yang

berhubungan dengan teknik enkripsi dan dekripsi dari algoritma *Rijndael* dan *Twofish*.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini membahas mengenai analisis kebutuhan dan perancangan. Analisis ini meliputi analisis algoritma *Rijndael* dan *Twofish*, analisis sistem, analisis kebutuhan fungsional, analisis spesifikasi perangkat yang terdiri dari spesifikasi kebutuhan perangkat lunak, spesifikasi perangkat keras. Kemudian juga akan dibahas mengenai perancangan perangkat lunak, yang meliputi perancangan antarmuka dan perancangan prosedural.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Berisi tentang tahapan implementasi sistem yang meliputi implementasi perangkat lunak, implementasi perangkat keras, implementasi basisdata, dan implementasi antarmuka. Untuk tahapan pengujian sistem ini menggunakan pengujian *alpha* yang meliputi metode pengujian, rencana pengujian, kasus dan hasil pengujian.

BAB 5 KESIMPULAN DAN SARAN

Berisi kesimpulan hasil pengujian *alpha* dan hasil pengujian data atau sistem serta saran yang dapat memberikan perbaikan sistem yang telah dibuat guna memperoleh kesempurnaan sistem.