BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang begitu pesat, khususnya dibidang teknologi informasi yang memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi atau data. Seiring dengan kemajuan teknologi informasi maka sangatlah diperlukan sebuah sekuritas atau keamanan terhadap kerahasiaan sebuah informasi atau data yang saling dipertukarkan. Dalam hal ini komunikasi atau pertukaran data yang menggunakan layanan media jaringan komputer *Local Area Network* (LAN) , karena dengan menggunakan media jaringan komputer *Local Area Network* (LAN) dapat berbagi atau bertukar data antara seorang *user* dengan *user* yang lain dalam satu areal yang terkoneksi jaringan komputer *Local Area Network* (LAN). Oleh karena itu didalam dunia informatika dikenal dengan cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau lebih dikenal dengan istilah Kriptografi.

Didalam keamanan jaringan komputer khususnya jaringan komputer *Local Area Network* (LAN). Memungkinkan untuk berbagi dan *sharing document* penting dengan *user* yang lainnya. Maka untuk mengamankan *document* atau data yang bersifat penting dan mengatasi hal – hal diatas diperlukannya sebuah cara untuk mengamankan suatu data atau informasi dengan menggunakan teknik kriptografi. Saat ini sudah banyak berkembang algoritma kriptografi yang mendukung untuk mengamankan suatu data atau informasi yang kita punya dari

orang atau pihak yang tidak berhak untuk mengakses data atau informasi tersebut. Didalam ilmu kriptografi *modern* dikenal dengan algoritma kriptografi *Blowfish* dan *Twofish,* keduanya dirancang oleh orang yang sama yaitu Bruce Schneier. Namun keduanya berasal dari masa yang berbeda. *Blowfish* merupakan algoritma yang lebih tua, ia dirancang pada tahun 1993, sedangkan *Twofish* tahun 1997.

kedua algoritma tersebut termasuk dalam kategori kunci *Chiper* 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. Seperti yang diungkapkan oleh Bruce Scheneier [SCH95] dalam sebuah jurnal yaitu *Dr Dobb's Journal* yang berjudul *Encryption Algorhitm-One Year Later* diungkapkan bahwa *Blowfish* memiliki keunggulan dari beberapa algoritma kriptografi lainnya dari segi keamanan serta telah dianalisa dan diuji oleh beberapa *Cryptanalyst* kedalam beberapa sistem.

Dari latar belakang diatas penulis mencoba untuk membahas mengenai algoritma kriptografi *Blowfish* dan *Twofish,* dengan mengambil tema "**APLIKASI KEAMANAN PENGIRIMAN DATA PADA JARINGAN *LOCAL AREA NETWORK (LAN)* BERBASIS ALGORITMA KRIPTOGRAFI KOMBINASI BLOWFISH DAN TWOFISH".** Dalam tema skripsi ini membahas mengenai keamanan dalam pengiriman data melalui media jaringan *Local Area Network* (LAN) dengan menggunakan algoritma *Blowfish* dan *Twofish*.

1.2 Identifikasi Masalah

Identifikasi masalah dalam penulisan tugas akhir ini adalah bagaimana membangun aplikasi sebuah keamanan data dengan menggunakan algoritma kriptografi *Blowfish* dan *Twofish* pada saat proses enkripsi suatu data yang akan digunakan untuk keamanan pada saat pengiriman data melalui media jaringan *Local Area Network* (LAN).

1.3 Maksud Dan Tujuan

Maksud dari penulisan Tugas akhir ini adalah membuat sebuah aplikasi untuk kemanan pengiriman data dengan menggunakan algoritma kriptografi *Blowfish* dan *Twofish*.

Sedangkan tujuan dari penulisan Tugas Akhir ini adalah membuat aplikasi yang relatif aman didalam pengiriman suatu data pada jaringan *Local Area Network* (LAN).

1.4 Batasan Masalah

Adapun batasan masalah yang dapat dilakukan agar pembahasan ini lebih terarah, yaitu :

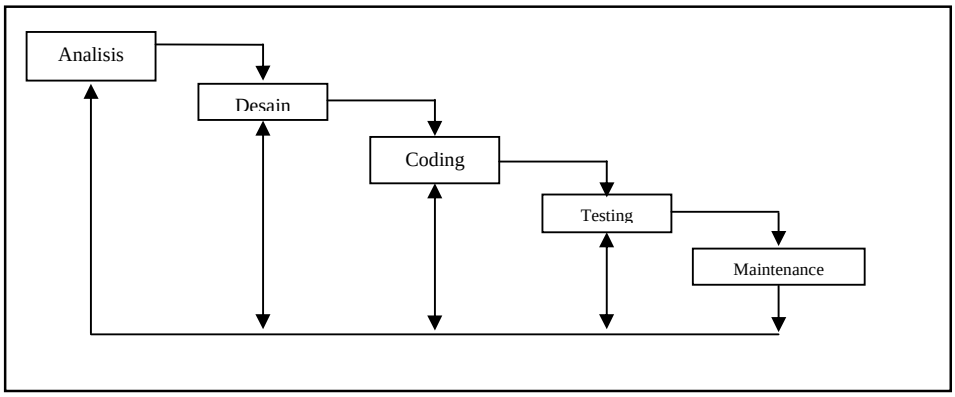
1. Algoritma kriptografi yang digunakan pada proses enkripsi dan dekripsi data adalah *Blowfish* 64 *bit* dan *Twofish* 128 *bit*.
2. Perangkat lunak (*Software*) yang digunakan dalam perancangan aplikasi adalah *Visual Basic 6.0.*
3. *Hardware* atau perangkat keras yang digunakan untuk pembuatan aplikasi ini adalah satu buah paket komputer dengan spesifikasi sebagai berikut:

a. Pentium III 800 Mhz
b. RAM 128 MB
c. *Hardisk* 10 GB
d. Kabel UTP (*Unshielded Twisted Pair*) dan konektor RG 45

4. Jenis data yang akan diuji enkripsi serta dekripsi yaitu jenis *file Txt, Doc,* JPG, Mp3 dan Mpeg.
5. Pengujian aplikasi di uji pada sebuah jaringan *Local Area Network* (LAN), dengan model hubungan *Peer to peer.*
6. Sistem operasi yang digunakan pada saat pengujian aplikasi yaitu menggunakan sistem operasi berbasis *Windows* XP.

1.5 Metodologi Penelitian

Metode yang digunakan untuk membahas kriptografi *Blowfish* dan *Twofish* ini adalah meliputi studi literatur dan pengumpulan data serta melakukan uji coba dari kriptografi *Blowfish* dan *Twofish* itu sendiri. Studi literatur digunakan untuk mempelajari dan memperdalam materi dasar dan terapan baik yang berkaitan dengan landasan teori maupun aplikasi. Pengumpulan data dilakukan dengan mengumpulkan data yang dibutuhkan dalam perancangan aplikasi. Perancangan Aplikasi yang dibangun sesuai dengan batasan yang telah ditentukan dengan menggunakan pendekatan terstruktur model "*Classic Life Cycle"* atau *waterfall* :



Gambar 1.1 Diagram *waterfall*

Keterangan Paradigma *Waterfall* sebagai berikut :

1. Tahap Analisis

   Kegiatan-kegiatan yang dilakukan pada tahap analisis ini yaitu mengumpulkan data dan menganalisa sistem.

2. Tahap Desain

   Kegiatan-kegiatan yang dilakukan pada tahap desain ini yaitu melakukan proses desain terhadap hasil yang didapat dari tahap analisis.

3. Tahap Pengkodean / *coding*

   Kegiatan-kegiatan yang dilakukan pada tahap pengkodean ini yaitu memulai dalam pembuatan program untuk membangun suatu sistem.

4. Tahap Ujicoba / *testing*

   Pada tahap ujicoba ini berisikan hal-hal yang mencakup pengujian program yang sudah dibuat.

5. Tahap Pemeliharaan / *maintenance*

   Pada tahap pemeliharaan ini berisikan hal pemeliharaan perangkat lunak (*software)* yang sudah tersedia agar dapat berjalan dengan baik.

1.6 Sistematika Penulisan

Untuk memberikan gambaran yang jelas mengenai penyusunan Tugas akhir ini, maka ditetapkan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, identifikasi masalah, maksud dan tujuan, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi tentang teori-teori yang melandasi dari permasalahan yang sedang dibahas.

BAB III ANALISIS DAN PERANCANGAN APLIKASI

Bab ini menjelaskan mengenai analisa dan rancangan dari aplikasi yang akan dirancang berdasarkan teori.

BAB IV IMPLEMENTASI APLIKASI

Bab ini berisi tahap implementasi dari sebuah aplikasi serta pengujian dari aplikasi yang telah dibuat.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang di dapat selama penulisan laporan tugas akhir dari pembahasan masalah, selain itu juga berisi saran untuk perbaikan dan menindak lanjuti hasil penelitian.