BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan suatu informasi menjadi hal yang sangat penting saat ini. Banyak orang kemudian berusaha untuk mencari cara bagaimana mengamankan informasi dalam melakukan pertukaran informasi. Salah satu caranya adalah dengan metode enkripsi menggunakan algoritma simetri. Namun terdapat kendala dalam penggunaan kunci untuk tipe algoritma simetri, dimana kunci yang digunakan untuk enkripsi dan dekripsi harus sama, sedangkan jika kunci untuk dekripsi dikirimkan terpisah akan menyebabkan kunci dapat diketahui dengan mudah oleh penyadap.

Pada penelitian sebelumnya [2], dilakukan penggabungan algoritma simetri dengan algoritma asimetri untuk keamanan dalam pengiriman data. Hal tersebut dilakukan agar kunci untuk proses dekripsi dapat dikirimkan dengan aman. Tetapi dengan penggabungan algoritma tersebut, maka akan berakibat proses yang dibutuhkan lebih lama. Untuk itu pada penelitian ini dirancang suatu sistem kemanan *file* menggunakan Algoritma Blowfish pada jaringan LAN. Kunci yang digunakan untuk enkripsi dan dekripsi akan disamarkan dan disisipkan bersama dengan data yang telah dienkripsi, hal ini dilakukan agar informasi kunci tidak dapat diketahui dengan mudah oleh penyadap. Setelah data yang telah dienkripsi dan dikirimkan sampai pada penerima, kunci yang telah disamarkan dan disisipkan akan diambil kembali dari data dan akan digunakan untuk proses dekripsi. Dengan begitu sistem ini lebih efektif karena hanya menggunakan satu algoritma untuk enkripsi dan dekripsi serta waktu proses akan lebih cepat dibandingkan penggabungan dengan algoritma asimetri.

1.2 Tujuan Penelitian

Tujuan yang ingin dicapai melalui penelitian ini adalah :

1. Merancang sebuah aplikasi enkripsi dan dekripsi *file* menggunakan Algoritma Blowfish dengan masukan berupa *file* teks, citra, suara dan video.

2. Mengimplementasikan sistem enkripsi menggunakan Algoritma Blowfish pada jaringan LAN dalam menjaga kerahasiaan data.

3. Menganalisa dan membandingkan kinerja Algoritma Blowfish dan Algoritma DES dari segi waktu enkripsi, waktu dekripsi, waktu pemecahan kunci dan *avalanche effect*.

1.3 Rumusan Masalah

Rumusan masalah dalam Tugas Akhir ini adalah:

1. Bagaimana proses enkripsi dan dekripsi *file* menggunakan Algoritma Blowfish.
2. Bagaimana proses pengiriman data pada jaringan LAN dengan kondisi data terenkripsi saat dikirimkan dan terdekripsi kembali saat diterima.

1.4 Batasan Masalah

Agar ruang lingkup masalah yang dibahas pada pengerjaan Tugas Akhir ini tidak terlalu luas maka dibutuhkan batasan masalah, diantaranya:

1. Program aplikasi yang dirancang menggunakan Algoritma Blowfish.
2. Informasi yang digunakan untuk pengiriman data, enkripsi dan dekripsi adalah *file* teks, citra, suara dan video.
3. Program yang digunakan untuk merancang aplikasi adalah Microsoft Visual Basic 2006.
4. Mode yang dipakai adalah Mode ECB (*Electronic Code Book*).
5. Algoritma pembanding yang digunakan adalah Algoritma DES.
6. Panjang kunci maksimal yang digunakan adalah 56 karakter atau 448 Bit.
7. Pengiriman data yang dilakukan melalui jaringan LAN dan menggunakan protokol TCP/IP.
8. Tidak membahas parameter-parameter jaringan.

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam pencapaian Tugas Akhir ini adalah :

1. Studi Literatur yang dilakukan untuk mempelajari konsep dasar dan teori pendukung yang berhubungan dengan permasalahan pada tugas akhir ini.

2. Pencarian data yang dilakukan sebagai bahan untuk proses analisa. Data yang digunakan adalah *file* teks, citra, suara dan video.

3. Merancang program aplikasi pada software Microsoft Visual Basic 2006 yang akan digunakan untuk pengimplementasian Tugas Akhir ini.
4. Menganalisa data yang telah didapat dengan program aplikasi sesuai dengan parameter yang telah ditentukan.
5. Mengambil kesimpulan dari hasil analisa yang telah dilakukan dilihat dari parameter yang ada serta memberi saran untuk penelitian selanjutnya.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Berisi latar belakang masalah, tujuan penelitian, rumusan masalah, batasan masalah, metodologi penelitian, serta sistematika penulisan Tugas Akhir ini.

BAB II DASAR TEORI

Berisi dasar-dasar teori yang diperlukan serta mendukung dalam penulisan Tugas Akhir ini.

BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM

Bab ini menjelaskan rancangan dari program aplikasi yang akan dibuat serta hal-hal lain yang akan digunakan sebagai dasar dari dibuatnya Tugas Akhir ini.

BAB IV PENGUJIAN SISTEM DAN ANALISA HASIL

Berisi analisa terhadap hasil yang diperoleh dari tahap perancangan dan implementasi sistem serta dilakukan pengujian terhadap sistem dari segi waktu enkripsi, waktu dekripsi, waktu pemecahan kunci dan *avalanche effect*. Kemudian akan dianalisa hasil dari pengujian tersebut.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan hasil penelitian dan saran-saran yang dapat digunakan untuk pengembangan Tugas Akhir ini selanjutnya.