BAB 1

PENDAHULUAN

1.1 Latar Belakang

Kata video berasal dari bahasa latin yang berarti “saya lihat”. Video adalah teknologi pemrosesan sinyal elektronik yang mewakili gambar bergerak. Dalam buku yang berjudul Multimedia Digital – Dasar Teori dan Pengembangannya, dijelaskan bahwa video sudah menjadi bagian dalam kehidupan sehari-hari. Aplikasi video seperti *video-on-demand, video broadcast dan video conference* merupakan beberapa contoh dari sekian banyak penerapan video dalam kehidupan sehari-hari (Binanto, 2010).

Terjadi banyak ancaman pencurian atas informasi data yang berlangsung tanpa kita sadari. Dalam buku pengantar ilmu kriptografi teori analisis dan implementasi oleh Doni Ariyus disebutkan bahwa ancaman seperti *Interruption* atau pengerusakan data, *Interception* atau penyadapan, *Modification* atau manipulasi data dan *Fabrication* atau data palsu merupakan ancaman yang sering terjadi atas informasi data. Berbekal dari permasalahan tersebut, banyak metode yang dikembangkan untuk mengatasi berbagai permasalahan keamanan dalam komunikasi informasi. Kriptografi adalah salah satu cara yang efektif untuk mengatasi ancaman-ancaman terhadap keamanan informasi data, dengan cara menyamarkan isi dari informasi yang hendak dikirimkan. Dalam buku yang berjudul Anti Forensik Mengatasi Investigasi Komputer Forensik yang ditulis Eko Arryawan dan SmitDev Community, diterangkan bahwa kerahasiaan data merupakan tujuan utama dari kriptografi, sehingga meskipun data dicuri, infromasinya tidak dapat dibaca karena telah disandikan atau dikodekan dengan metode tertentu (Ariyus, 2008).

Ancaman pelanggaran dalam bidang hak cipta disamping telah merugikan Negara sebagai akibat kehilangan pajak, juga telah merugikan si pencipta atau pemilik hak cipta. Sehingga diperlukan metode untuk melindungi hak cipta tersebut (Handoko, 2009).

John R.Vacca dalam bukunya yang berjudul *COMPUTER AND INFORMATION SECURITY*, menguraikan bahwa Ilmu kriptografi adalah ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dibaca oleh orang yang tidak berkepentingan. Kriptografi sudah dipakai sejak jaman Julius Caesar dimana akan mengirimkan pesan kepada panglimanya tetapi tidak mempercayai kurir pembawa pesan tersebut. Kriptografi mempunyai dua bagian yang penting, yaitu enkripsi dan dekripsi. Enkripsi adalah proses dari penyandian pesan asli menjadi pesan yang tidak dapat diartikan seperti aslinya. Dekripsi sendiri berarti merubah pesan yang sudah disandikan menjadi pesan aslinya. Pesan asli biasanya disebut *plaintext*, sedangkan pesan yang sudah disandikan disebut *ciphertext* (John, 2009).

Pada kesempatan ini, penulis mencoba menerapkan kriptografi dengan cara melakukan enkripsi menggunakan algoritma DES untuk meningkatkan keamanan data khususnya pada file video. Sehingga penulis mengambil judul "**Penerapan Algoritma DES untuk Enkripsi dan Dekripsi pada file video**", dengan tujuan untuk meningkatkan keamanan data video.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang sebagaimana yang telah diuraikan sebelumnya, rumusan masalah yang disimpulkan oleh penulis adalah: "Bagaimana menerapkan algoritma DES untuk enkripsi dan dekripsi pada file video?"

1.3 Batasan Masalah

Dalam penelitian ini penulis memberi batasan, antara lain:

1. File yang akan dienkripsi adalah file video dengan kapasitas 1MB
2. Fitur enkripsi dan dekripsi menggunakan algoritma DES

1.4 Tujuan Penelitian

Tujuan penyusunan tugas akhir ini adalah bagaimana menerapkan algoritma DES untuk enkripsi dan dekripsi pada file video.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini, antara lain:

1. Meningkatkan keamanan informasi data video.
2. Mengurangi resiko manipulasi data video oleh pihak lain.

1.6 Metodologi Penulisan Seminar Tugas Akhir

Dalam pembuatannya, Penulis melakukan beberapa penerapan metode penelitian untuk menyelesaikan permasalahan. Metode analisis dan desain yang akan penulis gunakan dalam penelitian ini adalah metode air terjun atau sering disebut *Waterfall* (Sommerville, 2003).

1. Analisis Kebutuhan

   Pada tahap ini dimulai dengan mengumpulkan bahan, mulai dari metode dan algoritma yang akan digunakan
2. Perancangan

   Merancang prosedur kerja dari media yang akan dibangun, sesuai dengan algoritma yang digunakan.
3. Implementasi

   Menerapkan enkripsi dan dekripsi sesuai dengan prosedur hasil perancangan dengan menggunakan bahasa pemrograman php.
4. Pengujian

   Pengujian dilakukan untuk mengetahui integritas data yang dienkripsi .

1.7 Sistematika Penulisan Seminar Tugas Akhir

Untuk memberikan gambaran secara garis besar mengenai pembahasan tiap bab yang terdapat dalam seminar tugas akhir, berikut akan diuraikan secara singkat sistematika penulisannya, antara lain :

BAB 1 PENDAHULUAN

Pada bab ini, membahas mengenai latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat seminar tugas akhir, metodologi penelitian, serta sistematika penulisan seminar tugas akhir.

BAB 2 LANDASAN TEORI

Dalam bab ini dibahas mengenai beberapa teori yang dipakai untuk mendukung penulisan seminar tugas akhir.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini menguraikan kebutuhan dasar yang diperlukan selama proses pengembangan perangkat lunak, meliputi pembahasan mengenai algoritma DES serta prosedur kerjanya, serta menguraikan tentang gambaran secara umum dari desain dan tampilan-tampilan perangkat lunak yang dibangun.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Bab ini, berupa penjelasan mengenai tahap realisasi setiap prosedur yang telah dirancang ke dalam bentuk program, serta pengujian yang dilakukan terhadap perangkat lunak yang dibangun.

BAB 5 PENUTUP

Bab ini berisi kesimpulan secara umum dan saran yang diharapkan dapat membangun di masa yang akan datang.