

BAB I

PENDAHULUAN

1.1 Latar Belakang

Informasi menjadi hal penting yang tidak bisa lepas dari kehidupan sosial manusia. Bahkan tujuan utama aktivitas komunikasi yang menjadi jembatan interaksi antar-individu adalah adanya pertukaran informasi. Hal ini menunjukkan betapa pentingnya kedudukan informasi dalam kehidupan sehari-hari.

Saat ini, proses tukar informasi menjadi lebih mudah. Namun, diantara informasi-informasi tersebut, tidak semua berhak diketahui khalayak umum. Demi menjaga keutuhan dan kerahasiaan data informasi tersebut, pengamanan data tentu menjadi barang penting. Pengamanan data ini dikenal dengan sebutan kriptografi.

Kriptografi bisa disebut sebagai seni atau ilmu penyandian untuk menyembunyikan data asli dari pihak-pihak yang tidak memiliki wewenang dalam pengaksesan data tersebut, entah itu pihak yang memang berniat menyerang data maupun pihak-pihak lain yang nantinya berpotensi membahayakan data yang dibagikan tersebut. Data yang dilindungi dengan kriptografi dapat berbentuk data apapun seperti audio, teks, citra digital, atau video yang nantinya akan di enkripsi saat transmisi data maupun pada penyimpanan data tersebut (Abomhara et al. 2009).

Sebagaimana telah disebutkan bahwa informasi dapat berbentuk data apapun, salah satunya yaitu data berupa video. Laju transfer dan pengaksesan video saat ini semakin cepat dengan makin besarnya kapasitas bandwidth serta makin banyaknya perangkat berkapasitas besar yang memungkinkan pengambilan data secara *real-time*.

Sistem pengamanan data video telah banyak dikembangkan dengan menggunakan berbagai teknik yang berbeda demi membangun sistem yang tangguh terhadap serangan dan juga efisien dari segi waktu maupun kebutuhan *storage* nya. Dari berbagai algoritma yang telah diterapkan pada sistem sejenis, kebanyakan yang digunakan adalah algoritma yang memang dikhususkan untuk kriptografi video seperti *Video Encryption Algorithm* (VEA), DES maupun RSA.

Dalam kriptografi terdapat berbagai algoritma yang telah dikembangkan. Salah satunya adalah Algoritma Camellia, yang masih jarang digunakan untuk implementasi pada kriptografi video. Oleh karena itu, penelitian ini akan mencoba untuk menerapkan Algoritma Camellia pada sistem kriptografi video.

1.2 Perumusan Masalah

Perumusan masalah pada penelitian ini adalah sebagai berikut

1. Bagaimana penerapan Algoritma Camellia pada kriptografi video?
2. Bagaimana kualitas kriptografi video menggunakan Algoritma Camellia?

1.3 Pembatasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut :

1. Algoritma kriptografi yang digunakan dalam pembuatan sistem adalah Algoritma Camellia.
2. Video yang digunakan sebagai data uji pada simulasi maksimal 5 detik dengan *frame rate* tidak lebih dari 30 fps.
3. Kunci yang digunakan sebesar 128 bit.

1.4 Tujuan

Adapun tujuan penelitian yaitu membuat sebuah sistem kriptografi video dengan Algoritma Camellia sebagai metodenya, serta mengetahui performa algoritma tersebut pada proses enkripsi dekripsi data video.

1.5 Manfaat

Hasil penelitian dapat menjadi referensi untuk mempertimbangkan penggunaan Algoritma Camellia pada kriptografi video serta mengembangkannya pada penelitian di masa mendatang.

1.6 Sistematika Penulisan

Laporan tugas akhir ini terdiri atas lima bab, berikut adalah sistematika penulisan beserta penjelasan singkat mengenai masing-masing bab :

BAB I PENDAHULUAN

Bab ini, menjelaskan latar belakang pembuatan sistem, perumusan masalah, pembatasan masalah dalam pembuatan sistem, tujuan pembuatan sistem, manfaat pembuatan sistem, dan sistematika penulisan laporan.

BAB II LANDASAN TEORI

Bab ini penulis memaparkan landasan teori yang digunakan sebagai penunjang untuk membuat tugas akhir ini.

BAB III ANALISA DAN PERANCANGAN PROGRAM

Bab ini berisi mengenai analisa bisnis proses, perancangan diagram konteks dan *data flow diagram*, perancangan *database*, serta desain *user interface*.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi tentang penerapan sistem dan tampilan sistem secara umum, serta hasil pengujian sistem.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan dan saran dari peneliti terhadap penelitian yang telah dilakukan.