ABSTRAKSI

Dengan pesatnya perkembangan teknologi di bidang telekomunikasi, suatu informasi memerlukan suatu keamanan dan kerahasian karena informasi itu menjadi barang yang sangat berharga sekali. Salah satu cara untuk mengamankan data tersebut adalah dengan menggunakan kriptografi. Kriptografi itu sendiri adalah cabang ilmu matematika yang memanfaatkan proses komputasi untuk mengacak data yang bertujuan untuk mencegah pihak-pihak yang tidak di izinkan untuk mengetahui dan memodifikasi data-data tersebut.

Pada kriptografi terdapat enkripsi dan dekripsi. Enkripsi adalah proses mengubah data asli (*plaintext*) kedalam bentuk yang tidak dapat dibaca (*ciphertext*) dengan menggunakan suatu kunci dan dekripsi adalah proses mengubah data yang sudah dalam bentuk tidak dapat dibaca *(ciphertext)* kedalam bentuk yang dapat dibaca kembali (*plaintext*) dengan menggunakan sebuah kunci. Untuk dapat melakukan enkripsi dan dekripsi dibutuhkan algoritma dan kunci.

Dalam tugas ini dibuat perancangan dan diteliti simulasi video enkripsi dan dekripsi tersebut dengan menggunakan format .AVI tanpa terkompresi dan tanpa suara. Pengenkripsian video dilakukan dengan byte-byte dimana byte adalah unit dasar dari operasi yang akan dilakukan pada blok data dari tiap-tiap frame yang terdiri dari 3 layer dengan menambahkan kriptografi kunci rahasia AES (*Advance Encryption Standard*) 128 bit *block cipher* yang simetrik dan di *hash* dengan SHA-1 sebagai pembangkit kunci untuk enkripsi dan dekripsi.

Dari penelitian maka algoritma AES 128 bit dan pembangkit kunci SHA-1 untuk *file* video bahwa algoritma AES memiliki tingkat keamanan yang tinggi karena memiliki *avalanche effect* yang baik, waktu *brute force attack* yang relatifcukup lama dan SHA-1 memiliki nilai variansi yang kecil.

Kata kunci : Enkripsi dan dekripsi video, AES 128 bit, pembangkit kunci SHA-1