

Abstrak

Tugas Akhir ini membahas perancangan keamanan video dengan menerapkan metode enkripsi selektif dalam mengamankan data video. Pada umumnya, data video memiliki nilai yang lebih rendah dibandingkan dengan data digital lainnya (seperti data rahasia pada sebuah perusahaan, informasi bank, dll). Maka dari itu enkripsi selektif dipilih dalam mengamankan data video karena enkripsi selektif adalah salah satu metode yang dapat mengatasi permasalahan performansi. Enkripsi selektif merupakan sebuah teknik untuk mengenkripsi sebagian porsi dari data video, sedangkan data lainnya dibiarkan sebagaimana adanya. Enkripsi dilakukan dengan algoritma RSA, salah satu dari *public-key cryptosystem* yang sangat sering digunakan untuk memberikan privasi terhadap keaslian suatu data digital. Keamanan enkripsi/dekripsi data model ini terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar.

MPEG-1 dan MPEG-2 merupakan format video yang digunakan pada tugas akhir ini, karena kedua format tersebut memiliki struktur *bitstream* yang hampir sama, sehingga pemrosesannya dapat dilakukan dengan satu algoritma. Data visual yang akan dienkripsi adalah pada lapisan *picture* yaitu *frame I* dan *frame P*. keamanan video dapat dicapai dengan mengenkripsi data ini.

Pada tugas akhir ini akan dibangun sebuah perangkat lunak dengan menggunakan *platform* Java berdasarkan perancangan. Pengujian yang dilakukan yaitu dengan mengenkripsi dan mendekripsi video dengan format MPEG-1 dan MPEG-2. Hasil pengujian menguji bahwa keamanan video dapat direalisasikan dengan menggunakan metode enkripsi selektif dan *key length* pada algoritma RSA yang sesuai untuk diimplementasikan dan sesuai dengan kebutuhan yang dapat dilihat pada parameter *Brute Force Attack*.

Kata kunci : *Video MPEG, Kriptografi, Selektif, RSA, Brute Force Attack*