

ABSTRAK

Perkembangan teknologi informasi yang sangat pesat dewasa ini menyebabkan informasi menjadi suatu hal yang sangat berharga, oleh karena itu perlu dilakukan perlindungan terhadap informasi dengan pelbagai cara. Salah satu cara lazim untuk melindungi data adalah kriptografi. Kriptografi sendiri merupakan cabang dalam ilmu matematika yang memanfaatkan proses komputasi untuk mengacak data, yang bertujuan untuk mencegah pihak-pihak yang tidak diizinkan untuk mengetahui atau memodifikasi data tersebut.

Tugas akhir ini menggunakan algoritma simetrik AES, dimana pada algoritma simetri mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu sebelum mereka dapat berkomunikasi dengan aman. Keamanan algoritma simetri tergantung pada kunci. Agar komunikasi tetap aman, kunci harus tetap dirahasiakan.

Pada tugas akhir ini, mengimplementasikan penggunaan algoritma simetrik AES untuk mengenkripsi/mendekripsi sebagian citra digital yang dianggap penting oleh user saja, sehingga lebih cepat dalam hal waktu proses operasi enkripsi/dekripsinya. Citra akan dipotong(*crop*) terlebih dahulu sebelum dilakukan proses kriptografi terhadap citra hasil *cropping* tersebut. Citra hasil pengacakan(*cipher*) akan ditempatkan lagi ke posisi citra asli(*plain*) sehingga menjadi citra yang utuh kembali. Untuk proses dekripsi adalah kebalikan dari proses enkripsi.

Dalam hal *brute forced attack*, tingkat keamanan untuk citra ukuran yang lebih besar dari 20x20 pixel lebih aman dibandingkan citra ukuran 20x20 pixel. Waktu proses untuk citra dengan ukuran 20x20 pixel lebih cepat dibandingkan citra dengan ukuran yang lebih besar dan citra satu layer lebih cepat dibandingkan dengan citra tiga layer. Hasil dari implementasi ini adalah sistem ini mampu melakukan proses enkripsi/dekripsi sebagian citra digital dalam waktu proses yang cepat dan tingkat keamanan yang tinggi. Dapat mengimplementasikan enkripsi pada sebagian citra digital dengan menggunakan algoritma AES.

Kata kunci: Enkripsi, Dekripsi, Citra, AES, *Cropping*.