ABSTRAK

AES (*Advanced Encryption Standard*) adalah salah satu algoritma enkripsi yang modern yang populer dan banyak digunakan. Algoritma ini adalah algoritma *block cipher 128 bit*, dengan kunci simetris berukuran *128 bit, 192 bit*, dan *256 bit*. Mode *ECB* dan *CBC* adalah dua mode operasi yang umum digunakan dalam enkripsi dengan AES, kedua mode ini memiliki karakteristik yang berbeda dalam hal tingkat keamanan dan waktu untuk enkripsi. Dalam penelitian ini penulis melakukan serangkaian percobaan untuk mengukur tingkat keamanan menggunakan *Avalanche Effect* dan waktu enkripsi diperoleh dari rata-rata waktu enkripsi dalam percobaan, percobaan dimulai dari menggunakan plaintext yang yang sama dengan key berbeda, percobaan berikutnya menggunakan plaintext yang berbeda dengan key yang sama. Pengujian ini menggunakan beberapa ukuran paintext yang berbeda, sedangkan kunci dengan ukuran tetap. Tujuan penelitian ini adalah untuk membandingkan tingkat keamanan yang dicapai oleh *ECB* dan *CBC*, serta waktu untuk melakukan enkripsi dari kedua mode ini.

Penelitian ini diharapkan dapat memberikan pemahaman yang lebih baik dalam memilih mode operasi yang sesuai dengan kebutuhan mode *ECB* dan *CBC* dalam hal keamanan dan juga waktu enkripsi.

Kata Kunci : Aes, Ecb, Cbc, Avalanche Effect, Enkripsi

ABSTRACT

AES (*Advanced Encryption Standard*) is a popular and widely used modern encryption algorithm. It is a *128-bit block cipher* algorithm with symmetric keys of sizes *128 bits, 192 bits,* and 256 bits. *ECB and CBC* modes are two commonly used modes of operation in AES encryption. These modes have different characteristics in terms of security level and encryption time. In this research, the author conducted a series of experiments to measure the security level using the *avalanche effect,* and the encryption time was obtained from the average encryption time in the experiments. The experiments started by using the same plaintext with different keys, followed by using different plaintexts with the same key. The testing involved various sizes of plaintext, while the key size remained fixed. The aim of this study is to compare the security level achieved by *ECB* and *CBC,* as well as the encryption time of both modes. This research is expected to provide a better understanding in selecting the appropriate mode of operation, either *ECB* or *CBC,* based on security and encryption time requirements.

Keywords : Aes, Ecb, Cbc, Avalanche Effect, Encryption.