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 CFB 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 ratarata 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, sedangkan untuk waktu enkripsinya, berbagai ukuran *plaintext* digunakan, sementara ukuran *key* tetap pada 128bit.

Tujuan utama adalah untuk membandingkan tingkat keamanan yang dicapai oleh ECB dan CFB, 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 CFB dalam hal keamanan dan efisiensi waktu.

Kata kunci: Kriptografi, AES, ECB, CFB, *Avalanche Effect*, Enkripsi

ABSTRACT

AES (Advanced Encryption Standard) is one of the modern and widely used encryption algorithms. It is a 128-bit block cipher algorithm with symmetric keys of sizes 128 bits, 192 bits, and 256 bits. ECB (Electronic Codebook) and CFB (Cipher Block Chaining) 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 encryption time obtained from the average encryption time in the experiments. The experiments started by using the same plaintext with different keys, and the next experiments used different plaintext with the same key. As for the encryption time, different sizes of plaintext were used, while the key size remained fixed at 128 bits.

The main objective is to compare the security levels achieved by ECB and CFB, as well as the time taken to perform encryption in both modes. This research aims to provide a better understanding in choosing the appropriate mode of operation between ECB and CFB in terms of security and time efficiency.

Keywords: *Cryptography, AES, ECB, CFB, Avalanche Effect, Enkripsi*