ABSTRAK

Keamanan data dalam komunikasi suara digital menjadi perhatian penting di era teknologi saat ini. Algoritma Advanced Encryption Standard (AES) merupakan salah satu algoritma kriptografi simetris yang banyak digunakan karena tingkat keamanannya yang tinggi. Penelitian ini bertujuan untuk menganalisis tingkat keamanan algoritma AES pada data audio digital, khususnya dengan mode operasi Electronic Codebook (ECB), serta membandingkannya dengan mode Cipher Block Chaining (CBC). Data audio berupa tiga jenis suara (burung, manusia, dan drum) dalam format WAV dienkripsi menggunakan AES dengan panjang kunci 128, 192, dan 256-bit. Evaluasi dilakukan melalui analisis histogram, cross-correlation, dan euclidean distance untuk menilai tingkat keacakan dan perbedaan antara sinyal asli dan sinyal terenkripsi. Hasil penelitian menunjukkan bahwa mode CBC memberikan hasil enkripsi yang lebih acak dan menyamarkan pola sinyal asli secara lebih efektif dibandingkan ECB. Dengan demikian, mode CBC direkomendasikan untuk penerapan enkripsi pada data audio karena mampu memberikan tingkat keamanan yang lebih baik.

Kata kunci: kriptografi, AES, ECB, CBC, enkripsi audio, histogram, cross-correlation, euclidean distance

ABSTRACT

Data security in digital voice communication is a major concern in today's technological era. The Advanced Encryption Standard (AES) algorithm is one of the most widely used symmetric cryptography algorithms due to its high level of security. This study aims to analyze the security level of the AES algorithm on digital audio data, particularly using the Electronic Codebook (ECB) mode, and compare it with the Cipher Block Chaining (CBC) mode. The audio data consists of three types of sounds (bird, human, and drum) in WAV format, encrypted using AES with key lengths of 128, 192, and 256 bits. The evaluation was conducted through histogram analysis, cross-correlation, and Euclidean distance to assess the level of randomness and differences between the original signal and the encrypted signal. The results of the study indicate that the CBC mode provides more random encryption results and more effectively masks the original signal pattern compared to ECB. Therefore, the CBC mode is recommended for encryption applications on audio data as it provides a higher level of security.

Keywords: cryptography, AES, ECB, CBC, audio encryption, histogram, cross-correlation, Euclidean distance