ABSTRAK

Kriptografi adalah ilmu yang berfungsi dalam melindungi data yang mengubah bentuknya mulai dari bentuk yang dapat dipahami menjadi tidak dapat dimengerti. Pada penelitian ini akan dilakukan pengujian pada suatu algoritma enkripsi simetris yaitu algoritma AES dengan menggunakan metode OFB yang akan dibandingkan dengan metode tanpa menggunakan *chain* yaitu ECB. Dari hasil enkripsi menggunakan kedua metode tersebut akan dibandingkan dengan menggunakan analisis histogram, nilai korelasi dan juga euclidean distance. Hasil penelitian menunjukkan bahwa metode OFB lebih menghasilkan kualitas enkripsi yang lebih baik dibandingkan dengan metode ECB dilihat dari analisis histogram yang menghasilkan grafik yang rata. Selain itu, nilai korelasi menghasilkan nilai yang lebih mendekati nol pada metode OFB, kemudian euclidean distance menghasilkan nilai yang besar dan juga mirip pada setiap gambarnya. Dilihat dari semua pengujian yang dilakukan, metode OFB lebih baik dibandingkan dengan metode ECB.

Kata Kunci: Kriptografi, Algoritma AES, OFB, *Output Feedback*

ABSTRACT

Cryptography is a science that functions in protecting data that changes its form from an understandable to an incomprehensible form. In this study, testing will be carried out on an symmetrical encryption algorithm, namely the AES algorithm using the OFB method which will be compared with a method without using a chain, namely ECB. The encryption results using the two methods will be compared using histogram analysis, correlation values and also euclidean distance. The results show that the OFB method produces better encryption quality compared to the ECB method as seen from the histogram analysis which produces a flat graph. In addition, the correlation value produces a value closer to zero in the OFB method, then the euclidean distance produces a large value and is also similar in each image. Judging from all the tests conducted, the OFB method is better than the ECB method.

Kata Kunci: Cryptography, AES Algorithm, OFB, *Output Feedback*