ABSTRAK

Advanced Encryption Standard (AES) merupakan algoritma enkripsi simetris yang umumnya digunakan untuk melindungi data digital. Namun, tantangan terkait penyimpanan dan pengiriman pesan terenkripsi melalui *platform website* tetap ada. Selain itu, kekhawatiran akan potensi serangan terhadap kunci kriptografi serta pengembangan metode kriptanalisis semakin memperkuat kebutuhan akan peningkatan keamanan. Penelitian ini bertujuan untuk menggabungkan dua teknologi, yaitu kriptografi *Advanced Encryption Standard* (AES) dengan modifikasi pada *SubBytes*, dan steganografi menggunakan metode *Least Significant Bit* (LSB) pada gambar, untuk meningkatkan tingkat keamanan pesan terenkripsi dalam konteks pengiriman melalui *website*. Dalam penelitian ini, dilakukan modifikasi terhadap algoritma AES dengan mengganti S-*box* pada proses *SubBytes* dengan *perfect* SAC S-*box* yang memiliki nilai rata-rata SAC sebesar 0,5. Aplikasi yang dihasilkan dibangun menggunakan *framework Streamlit* dengan menggunakan metode pengembangan *Waterfall*. Pengujian ini terbagi menjadi dua jenis, yaitu pengujian algoritma dan pengujian sistem. Pengujian algoritma melibatkan metode uji performa yang menunjukkan waktu dekripsi yang lebih lama dengan rata-rata selisih sebesar 80.27 milidetik, uji *cryptanalysis* yang menunjukkan peningkatan keamanan *ciphertext* berdasarkan estimasi waktu *cryptanalysis* menggunakan *brute force*, dan uji *randomness* untuk menunjukkan peningkatan pada tes *Frequency* dan *Poker*. Pengujian sistem menggunakan metode *Black Box* menunjukkan hasil yang valid sesuai harapan.

Kata Kunci: *Advanced Encryption Standard*, *Least Significant Bit*, *SubBytes*, S-*box*

ABSTRACT

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm commonly used to protect digital data. However, challenges related to storing and transmitting encrypted messages through website platforms persist. Furthermore, concerns about potential attacks on cryptographic keys and the development of cryptanalysis methods further reinforce the need for security enhancement. This study aims to combine two technologies: the Advanced Encryption Standard (AES) cryptography with modifications to the SubBytes, and steganography using the Least Significant Bit (LSB) method in images, to enhance the security level of encrypted messages in the context of transmission through websites. In this study, modifications were made to the AES algorithm by replacing the S-box in the SubBytes process with a perfect SAC S-box with an average SAC value of 0.5. The resulting application was built using the Streamlit framework with the Waterfall development method. This testing is divided into two types: algorithm testing and system testing. Algorithm testing involves performance testing methods that show longer decryption times with an average difference of 80.27 milliseconds, cryptanalysis testing showing increased ciphertext security based on cryptanalysis time estimates using brute force, and randomness testing to demonstrate improvements in Frequency and Poker tests. System testing using the Black Box method shows results that are valid as expected.

Keywords: *Advanced Encryption Standard, Least Significant Bit, SubBytes, S-box*