ABSTRACT

In the midst of increasingly sophisticated cyber threats, a new approach is needed to secure digital files. One such approach is the combination of block cipher and stream cipher algorithms to maximize both security and efficiency. This study aims to implement and evaluate a modified AES algorithm by adding an AddRoundKey step before the MixColumns process and combining it with the ChaCha20 algorithm in a dual encryption scheme. This combination is referred to as "Mix," which integrates the modified AES algorithm and ChaCha20 to enhance data security. The method used involves testing on various file types (PDF, Word, TXT) of different sizes using the Python programming language. The evaluation was conducted on four algorithms: ChaCha20, standard AES, modified AES, and the Mix combination, using performance parameters including encryption time, decryption time, processing speed, and entropy value. Test results show that the modified AES algorithm produced an encryption time of 165.653 seconds, approximately 6% slower than standard AES. This modification increases encryption complexity due to the additional AddRoundKey step before MixColumns, thereby adding more XOR operations with the key and resulting in increased encryption time and decreased processing speed compared to standard AES. ChaCha20 had the fastest encryption time with an average of 0.019 seconds and a decryption time of 0.017 seconds. The combination of modified AES and ChaCha20 produced a high entropy value of 7.970, equivalent to that of ChaCha20. It can be concluded that the choice of algorithm should be adjusted according to the system's needs: efficiency, stability, or additional security.

***Keywords**: File Security, Advanced Encryption Standard (AES), ChaCha20, Double Encryption, AddRoundKey, Entropy*