ABSTRAK

Di tengah maraknya ancaman siber yang semakin canggih, dibutuhkan pendekatan baru dalam pengamanan *file* digital. Salah satu pendekatan yang dapat digunakan adalah kombinasi algoritma blok cipher dan stream cipher untuk memaksimalkan keamanan dan efisiensi. Penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi algoritma modifikasi AES dengan penambahan langkah *AddRoundKey* sebelum *MixColumns*, serta menggabungkannya dengan algoritma ChaCha20 dalam skema enkripsi ganda. Kombinasi ini disebut sebagai Mix, yaitu integrasi antara algoritma AES yang dimodifikasi dan ChaCha20 untuk meningkatkan keamanan data. Metode yang digunakan mencakup pengujian pada berbagai jenis *file* (PDF, Word, TXT) dengan ukuran berbeda, menggunakan bahasa pemrograman Python. Pengujian dilakukan terhadap empat algoritma: ChaCha20, AES standar, AES modifikasi, dan kombinasi *Mix*, dengan parameter evaluasi berupa waktu enkripsi, waktu dekripsi, kecepatan proses, dan nilai entropi. Hasil pengujian menunjukkan AES modifikasi menghasilkan waktu enkripsi sebesar 165.653 detik, hanya sekitar 6% lebih lambat dibandingkan AES standar. Modifikasi ini meningkatkan kompleksitas enkripsi karena penambahan langkah *AddRoundKey* sebelum *MixColumns*, sehingga menambah jumlah operasi XOR terhadap kunci dan berdampak pada peningkatan waktu enkripsi dan penurunan kecepatan proses dibandingkan AES standar. ChaCha20 memiliki waktu enkripsi tercepat dengan rata-rata 0.019 dan waktu dekripsi 0.017. Kombinasi AES modifikasi dan ChaCha20 menghasilkan entropi tinggi sebesar 7.970 yang setara dengan ChaCha20. Dapat disimpulkan bahwa pemilihan algoritma sebaiknya disesuaikan dengan kebutuhan: efisiensi, kestabilan, atau keamanan tambahan.

Kata Kunci: Keamanan *File*, *Advanced Encryption Standard* (*AES*), ChaCha20, Enkripsi Ganda, *AddRoundKey*, *Entropi*.