ABSTRAK

Keamanan data menjadi isu krusial di era digital, terutama bagi dokumen elektronik yang sering menjadi target serangan siber. Penelitian ini bertujuan mengembangkan sistem pengamanan file dokumen dengan masukan berupa file teks dan keluaran berupa file terenkripsi yang aman dari intersepsi pihak tidak sah. Meskipun algoritma seperti AES telah banyak digunakan, tantangan dalam pengelolaan kunci dan kebutuhan akan efisiensi tinggi di perangkat tanpa akselerasi hardware masih menjadi hambatan. Saat ini, sistem belum mampu menggabungkan kecepatan dan keamanan secara optimal, khususnya untuk file dengan berbagai ukuran. Penelitian ini mengusulkan metode hybrid kriptografi yang menggabungkan Diffie–Hellman sebagai algoritma pembentukan kunci rahasia dan ChaCha20 sebagai stream cipher untuk enkripsi data. Sistem ini memanfaatkan keunggulan Diffie–Hellman dalam pertukaran kunci aman serta efisiensi tinggi dari ChaCha20 dalam proses enkripsi dan dekripsi. Hasil menunjukkan bahwa kombinasi DH–ChaCha20 memiliki waktu enkripsi tercepat (0.1906 detik) dan throughput tertinggi (13651.4704 KB/s). Sistem ini terbukti unggul dalam kecepatan, efisiensi, dan ketahanan terhadap skenario file berukuran besar, menjadi solusi optimal dalam pengamanan file digital.

Kata Kunci: *ChaCha20, Diffie-Hellman, Efisiensi Enkripsi, Hybrid Kriptografi, Keamanan Data.*