# ABSTRAK

Dalam era digital, kebutuhan akan sistem berbagi file yang aman semakin penting, terutama pada lingkungan jaringan berbasis Linux. Penelitian ini mengusulkan sistem keamanan file menggunakan kombinasi algoritma enkripsi ChaCha20 dan modifikasi Advanced Encryption Standard (AES) melalui metode AddRoundKey. Sistem diimplementasikan pada protokol Server Message Block (SMB) versi 1 berbasis Samba dan dilengkapi antarmuka web client berbasis Flask untuk memfasilitasi unggah, unduh, serta pengelolaan file secara terenkripsi. Proses enkripsi dilakukan secara berlapis: data pertama-tama dienkripsi menggunakan AES modifikasi, kemudian hasilnya dienkripsi kembali dengan ChaCha20 untuk memperkuat keamanan terhadap serangan dan penyadapan.

Pengujian dilakukan terhadap berbagai jenis file teks dan gambar berukuran 10KB hingga 100MB untuk mengevaluasi performa sistem dari segi waktu enkripsi-dekripsi, kecepatan transfer, dan integritas data. Pengujian keamanan dilakukan melalui checksum dan analisis lalu lintas menggunakan Wireshark guna memastikan bahwa data tetap terlindungi selama proses transfer. Hasil pengujian menunjukkan bahwa rata-rata waktu enkripsi mencapai 0,02583 detik dan waktu dekripsi sebesar 0,02271 detik untuk file berukuran 1MB, serta file hasil dekripsi terbukti identik dengan file asli berdasarkan nilai hash checksum. Selain itu, histogram hasil enkripsi menunjukkan pola distribusi acak yang membuktikan efektivitas pengacakan data. Hasil tersebut menunjukkan bahwa kombinasi algoritma ini mampu memberikan perlindungan yang lebih baik dibandingkan metode Samba standar, serta mempertahankan integritas dan kerahasiaan file selama proses berbagi data. Sistem ini membuktikan efektivitas penerapan kriptografi hibrida dalam meningkatkan keamanan pada lingkungan file sharing berbasis protokol SMBv1.

**Kata Kunci**: ChaCha20, AES, AddRoundKey, Kriptografi Hibrida, Samba, SMBv1, Keamanan File, Wireshark