ABSTRAK

Di era digital yang semakin maju, keamanan informasi menjadi perhatian utama, terutama dalam melindungi dokumen sensitif dari ancaman siber. Kemajuan teknologi komputasi kuantum memunculkan tantangan baru terhadap kriptografi konvensional, seperti RSA dan AES. Penelitian ini mengusulkan sistem hybrid encryption yang menggabungkan algoritma Twofish dan Kyber Key Encapsulation Mechanism (KEM) untuk meningkatkan keamanan dokumen. Twofish, sebagai algoritma simetris, digunakan untuk efisiensi enkripsi data, sementara Kyber KEM, sebagai algoritma asimetris berbasis post-quantum, menangani pengelolaan kunci yang aman. Implementasi sistem ini mencakup tahapan key generation, encapsulation, enkripsi file, pengiriman data, decapsulation, hingga dekripsi file. Pengujian dilakukan terhadap berbagai ukuran file PDF dan DOCX mulai dari 100KB hingga 10MB. Hasil pengujian menunjukkan bahwa sistem mampu mengenkripsi dan mendekripsi file dengan cepat pada ukuran kecil hingga menengah. Sebagai contoh, file berukuran 1MB diproses dengan waktu total di bawah 1 detik, sedangkan file berukuran 10MB memerlukan waktu lebih dari 4 detik. Proses key generation menggunakan Kyber KEM juga menunjukkan waktu yang konsisten, rata-rata sekitar 0,2400 detik. Analisis hash value menunjukkan bahwa file hasil dekripsi identik dengan file asli, menandakan integritas data tetap terjaga. Selain itu, pengujian sniffing menggunakan Wireshark memperlihatkan bahwa isi data terenkripsi tidak dapat dibaca saat dikirim melalui jaringan, sehingga sistem dinyatakan aman terhadap serangan pihak ketiga. Dengan kombinasi ini, sistem hybrid encryption terbukti dapat diimplementasikan secara efektif dan mampu berfungsi dengan baik dalam proses perlindungan dokumen sensitif, terutama dalam menghadapi tantangan dari perkembangan teknologi kuantum di masa depan.

Kata Kunci: *Hybrid Encryption, Kyber KEM, Keamanan dokumen, Post-quantum cryptography, Twofish.*