ABSTRACT

In the increasingly advanced digital era, information security has become a major concern, especially in protecting sensitive documents from cyber threats. The emergence of quantum computing technology poses new challenges to conventional cryptographic algorithms such as RSA and AES. This study proposes a hybrid encryption system that combines the Twofish algorithm with the Kyber Key Encapsulation Mechanism (KEM) to enhance document security. Twofish, a symmetric algorithm, is used for efficient data encryption, while Kyber KEM, a post-quantum asymmetric algorithm, handles secure key encapsulation. The system implementation involves key generation, encapsulation, file encryption, data transmission, decapsulation, and file decryption. Testing was conducted on various file sizes, both PDF and DOCX, ranging from 100KB to 10MB. The results show that the system can encrypt and decrypt small to medium-sized files efficiently. For example, a 1MB file was processed in less than 1 second, while a 10MB file required more than 4 seconds. The key generation process using Kyber KEM was consistent, with an average duration of approximately 0.24 seconds. Hash value analysis confirmed that the decrypted file was identical to the original, indicating that data integrity was maintained. Additionally, sniffing tests using Wireshark showed that the encrypted data transmitted over the network was unreadable, proving that the system is secure against third-party interception. With this combination, the hybrid encryption system has been successfully implemented and is capable of functioning effectively in protecting sensitive documents, particularly in addressing future challenges posed by the advancement of quantum computing technology.

Keywords: *Document Security, Hybrid Encryption, Kyber KEM, Post-quantum cryptography, Twofish.*