INTISARI

Mekanisme Enkapsulasi Kunci Berbasis Modul Latis

Oleh

RICHARD TORMIN OCTAVIAN TOBING

20/455507/PA/19722

Beragam sistem kriptografi modern telah dikembangkan, salah satunya adalah sistem kriptografi berbasis *Learning With Errors* (LWE) oleh Regev. Perkembangan LWE telah mencapai ke tahap modul-LWE dan aplikasinya pada Mekanisme Enkapsulasi Kunci (KEM). Pada skripsi ini, akan dibahas Mekanisme Enkapsulasi Kunci berbasis modul-LWE (ML-KEM) dan fungsi hash SHA-3 sebagai bagian pada algoritma ML-KEM. Selain itu, terdapat simulasi program ML-KEM dengan parameter yang berbeda untuk melihat lama waktu yang dibutuhkan untuk mendapatkan kunci rahasia bersama. Melalui kajian ini, diharapkan dapat memberikan wawasan mendalam mengenai implementasi dan kinerja ML-KEM dalam kriptografi modern.

ABSTRACT

Module-Lattice-based Key-Encapsulation Mechanism

By

RICHARD TORMIN OCTAVIAN TOBING

20/455507/PA/19722

Various modern cryptographic systems have been developed, one of which is the cryptographic system based on *Learning With Errors* (LWE) by Regev. The development of LWE has reached the stage of module-LWE and its application to the Key Encapsulation Mechanism (KEM). This thesis discusses the Key Encapsulation Mechanism based on module-LWE (ML-KEM) and the SHA-3 hash function as part of the ML-KEM algorithm. Additionally, a simulation of the ML-KEM program with different parameters is presented to observe the time required to obtain a shared secret key. This study aims to provide in-depth insights into the implementation and performance of ML-KEM in modern cryptography.