ABSTRAK

Dalam era digital yang berkembang pesat, kebutuhan akan saluran komunikasi yang aman menjadi sangat penting. Kriptografi memainkan peran krusial dalam memastikan integritas dan kerahasiaan data. RSA (Rivest-Shamir-Adleman) adalah algoritma kriptografi asimetris yang dikenal luas untuk transmisi data yang aman, tetapi memiliki keterbatasan dalam manajemen kunci dan beban komputasi. Integrasi pendekatan *Diffie-Hellman* dengan RSA (DHRSA) diusulkan untuk mengatasi masalah ini, memungkinkan pertukaran kunci rahasia tanpa mentransmisikan kunci itu sendiri. Penelitian ini fokus pada integrasi algoritma RSA dengan pendekatan *Diffie-Hellman* untuk meningkatkan keamanan pertukaran kunci dalam komunikasi data sensitif. Analisis dilakukan terhadap kekuatan kunci yang dihasilkan dan potensi kerentanan yang diatasi. Hasil penelitian diharapkan memberikan pemahaman tentang bagaimana pendekatan ini dapat meningkatkan keamanan, efisiensi pertukaran kunci, dan latensi dalam komunikasi.

Kata Kunci : Kriptografi, RSA, *Diffie-Hellman*, Keamanan Data, Manajemen Kunci, Latensi Komunikasi.

ABSTRACT

In the rapidly evolving digital era, the need for secure communication channels is paramount. Cryptography plays a crucial role in ensuring data integrity and confidentiality. RSA (Rivest-Shamir-Adleman) is a widely known asymmetric cryptographic algorithm used for secure data transmission, but it has limitations in key management and computational load. Integrating the Diffie-Hellman approach with RSA (DHRSA) is proposed to address these issues, enabling the exchange of secret keys without transmitting the keys themselves. This study focuses on the integration of the RSA algorithm with the Diffie-Hellman approach to enhance key exchange security in sensitive data communication. The analysis is conducted on the strength of the generated keys and the potential vulnerabilities addressed. The research aims to provide insights into how this approach can improve security, key exchange efficiency, and communication latency.

Keywords : *Cryptography, RSA, Diffie-Hellman, Data Security, Key Management, Communication Latency.*