INTISARI

PENERAPAN NTRU SEBAGAI ALGORITMA *POST-QUANTUM CRYPTOGRAPHY* PADA APLIKASI PESAN INSTAN BERBASIS ENKRIPSI SECARA *END-TO-END*

Kriptografi menjadi salah satu bidang yang sangat penting bagi kehidupan digital saat ini. Salah satu jenis kriptografi yang penting di era sekarang ini adalah kriptografi kunci publik. Terdapat banyak kegunaan algoritma kriptografi kunci publik, salah satunya untuk melakukan komunikasi secara *end-to-end*. Sayangnya, fitur keamanan ini terancam oleh perkembangan komputer kuantum yang dikhawatirkan dapat merusak mayoritas algoritma kriptografi kunci publik.

Penelitian ini membahas tentang penggunaan algoritma kriptografi kunci publik yaitu NTRU yang aman dari serangan komputer kuantum sebagai sarana komunikasi yang aman secara *end-to-end*. Pada penelitian ini dibuat aplikasi pesan instan yang dapat menghubungkan dua pengguna untuk berkomunikasi secara langsung dan aman. NTRU digunakan sebagai algoritma utama penyusun skema *key encapsulation mechanism* yaitu skema yang digunakan untuk membangkitkan kunci simetris. Dilakukan juga analisis terkait efisiensi NTRU dan pemilihan parameter NTRU untuk mencegah adanya *decryption failure*.

Dari evaluasi terhadap aplikasi yang dibangun, didapatkan hasil bahwa NTRU lebih efisien waktu jika dibandingkan dengan RSA maupun X25519. Diperoleh juga rekomendasi metode pembangkitan pasangan kunci serta rekomendasi parameter NTRU.

Kata kunci : NTRU, *end-to-end*, aplikasi, pesan instan

ABSTRACT

NTRU AS POST-QUANTUM CRYPTOGRAPHY ALGORITHM IN END-TO-END ENCRYPTION-BASED INSTANT MESSAGING APPLICATION

Cryptography is an important field in current digital civilization. One of the most important type of cryptography is public key cryptosystem. There are many uses of public key cryptosystem, one of which is to perform end-to-end encrypted communication. Unfortunately, this security feature is threatened by the development of quantum computers which are feared to be able to break most public key cryptosystem algorithms.

This research discusses the use of one of the public key cryptosystem algorithms, NTRU, which is safe from quantum computer attacks. The NTRU is used to perform an end-to-end secure communication. In this research, an instant messaging application with the sole purpose of connecting two users to be able to communicate in real-time. NTRU is used as the main algorithm for the key encapsulation mechanism, which is the scheme used to generate a symmetric key for symmetric cryptosystem algorithm. Researcher also performed analysis related to the efficiency of NTRU and the selection of NTRU parameters to prevent decryption failure.

Evaluating the resulting application, it was found that NTRU is more efficient when compared to RSA and X25519. The research also produces recommendations for key pair generation methods and NTRU parameters.

Keyword : NTRU, *end-to-end*, application, *chatting*