ABSTRAK

Nama : Radja Iqbal Sanusi Harahap

Program Studi : Informatika

Judul : Implementasi Algoritma Diffie-Hellman Dan RSA-CRT Pada Aplikasi Chatting

Pembimbing 1 : Yusup Miftahuddin, S.Kom., MT

Pembimbing 2 : Nur Fitrianti Fahrudin, S.Kom., MT.

Penelitian ini bertujuan untuk melakukan penggabungan dua jenis algoritma yang berbeda yaitu *Diffie-Hellman* dan *RSA* untuk membangkitkan *public key* dan *privat key* yang digunakan untuk melakukan proses dekripsi dan enkripsi pada pesan. Melakukan perbandingan kecepatan waktu proses dekripsi dari algoritma *RSA* dengan algoritma *RSA* yang telah digabungkan dengan teorema *CRT* atau disebut *RSA-CRT*, dimana *CRT* dipilih untuk mempersingkat waktu proses dekripsi *RSA* yang tergolong lamban. Berdasarkan pengujian yang telah dilakukan menunjukkan bahwa, *RSA-CRT* mampu menyelesaikan proses dekripsi yang lebih cepat dibandingkan dengan *RSA*, dengan perbandingan waktu 16,590 *millisecond* lebih cepat pada panjang kunci dekripsi lima digit angka, 8407,295 *millisecond* lebih cepat pada panjang kunci dekripsi enam digit angka dan 1.244.411,270 *millisecond* lebih cepat pada panjang kunci dekripsi tujuh digit angka. Sehingga dapat disimpulkan bahwa algoritma *RSA-CRT* mampu melakukan proses dekripsi yang lebih cepat dibandingkan *RSA.*

Kata Kunci: Kriptografi, *Diffie-Hellman, RSA, RSA-CRT,* Aplikasi *Chatting*

ABSTRACT

Nama : Radja Iqbal Sanusi Harahap

Program Studi : Informatika

Judul : Implementasi Algoritma Diffie-Hellman Dan RSA-CRT Pada Aplikasi Chatting

Pembimbing 1 : Yusup Miftahuddin, S.Kom., MT

Pembimbing 2 : Nur Fitrianti Fahrudin, S.Kom., MT.

This study aims to combine two different types of algorithms, that are Diffie-Hellman and RSA to generate public and private keys that are used to decrypt and encrypt messages. Comparing the decryption process time speed of the RSA algorithm with the RSA algorithm that has been combined with the CRT theorem or called RSA-CRT, where the CRT was chosen to shorten the time the RSA decryption process was relatively slow. Based on the tests that have been carried out, it shows that RSA-CRT is able to complete the decryption process faster than RSA, with a time ratio of 16,590 *milliseconds faster at a five-digit decryption key length,* 8407,295 *milliseconds faster at a six-digit decryption key length, and* 1,244,411,270 *milliseconds faster at a seven-digit decryption key length. So it can be concluded that the RSA-CRT algorithm is able to perform a faster decryption process than RSA.*

Keywords : *Cryptography, Diffie-Hellman, RSA, RSA-CRT, Chatting Application*