ABSTRACT

One of public key algorithm is public key algorithm based on Diophantine equation introduced by C. C Chang and C. H. Lin on their journal titled "A New Public Key Ciphers System Based upon the Diophantine Equations" in 1995 [2]. Other public key algorithm commonly used is RSA (Riverst Shamir Adleman) [9]. Even though never been proved, RSA are considered as a secure algorithm for its high level of difficulties of factoring an enormous numbers, whereas algorithm based on Diophantine algorithm has least difficulties to find solutions. Although it is easy to find, the solution of Diophantine algorithm is possibly not the real solution since Diophantine equation [2] [4] usually has many solutions. It is harder to solve if there are more variable used.

On this final assignment, software is made to analyze Diophantine performance based on the number of key being used, compared with RSA certain bit algorithm. The parameters are key generation time, encryption and decryption time, and enlarged *ciphertext*.

The conclusions of performance comparison full analysis are Diophantine cryptography has encryption time performance 1 to 15 times and decryption time performance 3 to 41 times, faster than RSA. RSA generates *ciphertext* 1 to 6 times *plaintext* size while Diophantine cryptography generates *ciphertext* 1 to 4 times *plaintext* size. The analysis shows that encryption process of each algorithm on each kind of key needs almost 2 times of the decryption time. It also shows that the size of *plaintext* affects process duration and enlarged *ciphertext*. Bigger *plaintext* will cost more time of encryption and decryption, and makes *ciphertext* bigger for each algorithm on each kind of key used.

Keywords: cryptography, public key, Diophantine, RSA, *ciphertext*, *plaintext*, encryption, decryption.