# ABSTRAKSI

Salah satu algoritma kunci publik adalah kunci publik berbasis persamaan *Diophantine* yang pernah dikemukakan dalam jurnal oleh C. C Chang dan C. H. Lin berjudul *"A New Publik Key Chipher System Based Upon The Diophantine Equations*" pada tahun 1995 [2]. Algoritma kunci publik lain yang paling umum digunakan adalah RSA (**R**iverst **S**hamir **A**dleman) [9]. RSA dianggap aman karena sulitnya pemfaktoran bilangan yang sangat besar meskipun tidak pernah dibuktikan aman tidaknya. Sedangkan algoritma berbasis persamaan *Diophantine*, untuk menemukan solusinya cukup mudah, namun belum tentu solusi tersebut adalah solusi yang sebenarnya karena biasanya persamaan [2] [4] *Diophantine* memiliki solusi banyak, semakin banyak jumlah peubah yang digunakan semakin sulit untuk dipecahkan.

Pada Tugas Akhir (TA) ini dibuat sebuah perangkat lunak untuk menganalisis performansi algoritma *Diophantine* berdasar jumlah kunci yang digunakan dengan cara membandingkannya dengan algoritma RSA bit tertentu dengan beberapa parameter antara lain : waktu membangkitkan kunci, waktu enkripsi dan dekripsi, dan pembengkakan ukuran *ciphertext*.

Kesimpulan yang dapat diambil dari analisis perbandingan performansi secara keseluruhan adalah kriptografi Diophantine memiliki performansi waktu enkripsi 1 - 15 dan waktu dekripsi 3 - 41 kali lebih cepat dibanding RSA, RSA menghasilkan ukuran *ciphertext* 1 - 6 kali ukuran *plaintext*, sedangkan kriptografi Diophantine menghasilkan ukuran *ciphertext* 1 - 4 kali ukuran *plaintext*, proses enkripsi untuk setiap algoritma pada masing-masing jenis kunci memerlukan hampir 2 kali waktu dekripsinya, ukuran *plaintext* berpengaruh pada lamanya proses dan pembengkaan *ciphertext*. semakin besar ukuran *plaintext*, semakin lama proses enkripsi dan dekripsinya dan ukuran *ciphertext* juga semakin besar untuk setiap algoritma pada masing-masing jenis kunci yang digunakan

Kata Kunci : kriptografi, kunci publik, Diophantine, RSA, *ciphertext, plaintext*, enkripsi, dekripsi