ABSTRAKSI

Identity-Based Encryption memberikan kemudahan pada kriptografi dengan menggunakan sembarang *string* sebagai kunci publik. Pada kriptografi kunci publik, biasanya enkripsi menggunakan kunci publik yang rumit dan sulit diingat. *Identity-Based Encryption* menggunakan kunci yang lebih mudah di ingat. Kunci publik pada *Identity-Based Encryption* ini dapat berupa alamat email, nomor telepon, ataupun suatu kata. Dengan menggunakan metode ini, enkripsi dapat dilakukan sebelum mengetahui kunci privat dari pasangan kunci publik yang sesuai. Pada saat penerima menerima suatu pesan yang terenkripsi tersebut, penerima akan menghubungi *Private Key Generator* untuk mendapatkan kunci privat dari kunci publik yang digunakan dan mendekripsi pesan yang telah terenkripsi tersebut dengan menggunakan kunci privat yang didapat tersebut.

Identity Based Encryption yang dilakukan pada Tugas Akhir ini berdasar pada konsep yang dikenalkan oleh Boneh dan Franklin. Tugas Akhir ini berisi perancangan dan implementasi dari Identity Based Encryption Boneh Franklin dan perhitungan waktu terhadap fungsi-fungsi hasil implementasi dengan menggunakan perhitungan waktu pada sistem operasi.

Kata Kunci: Identity-Based Encryption, kunci publik, kunci privat, Private Key Generator.