ABSTRAK

Kriptosistem kurva elips (*elliptic curves cryptosystem*) merupakan salah satu sistem kriptografi asimetris yang menggunakan persoalan logaritma diskrit (*discrete logarithm problem*). Struktur kurva elips digunakan sebagai grup operasi matematis untuk melangsungkan proses enkripsi dan dekripsinya. Kunci yang digunakan adalah kunci asimetris. Pada Laporan Tugas Akhir ini diuraikan teknik dasar *Elliptic Curves Cryptosystem* (ECC) yang diimplementasikan pada protokol pertukaran kunci publik Diffie-Hellman dan skema enkripsi Elgamal. Pada pertukaran kunci, hasil implementasinya memperlihatkan pertukaran kunci publik antara dua *user* dan menghitungnya dimasing-masing *user* yang akan menghasilkan kunci rahasia bersama yang sama. Sementara pada skema enkripsi Elgamal, hasil implementasi telah menunjukkan pesan berupa karakter yang dipetakan dalam titik kurva yang kemudian dienkripsi berhasil dibuka kembali pada proses dekripsinya. Metodelogi yang dibangun adalah sistem yang mengubah plaintext menjadi chiptertext dengan munggunakan kunci asimetris dan didekripsi ulang menjadi plaintext awal. Dari hasil penelitian diperoleh tingkat keamanan data dengan menggunakan Algoritma *Elliptic curve crytosytem* lebih baik karena menggunakan kunci asimetris yaitu kunci yang berbeda pada proses enkripsi dan dekripsi ulang.

Kata kunci : *kriptografi, kurva elips, pertukaran kunci publik, Diffie-Hellman, skema enkripsi Elgamal.*