ABSTRAK

Wan Khudri, 2005. ENKRIPSI DAN DEKRIPSI DATA MENGGUNAKAN ALGORITMA ElGamal ECC (*ElGamal ELLIPTIC CURVE CRYPTOGRAPHY*). Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sebelas Maret.

Kriptografi adalah ilmu pengetahuan untuk menjaga keamanan informasi, termasuk didalamnya terdapat proses enkripsi dan dekripsi. Enkripsi adalah suatu proses untuk mengubah *plaintext* menjadi *chipertext* dan dekripsi adalah proses untuk mengembalikan *chipertext* menjadi *plaintext.* Algoritma yang digunakan dalam enkripsi dan dekripsi disebut algoritma kriptografi. Berdasarkan jenis kuncinya, algoritma kriptografi dibagi menjadi dua, yaitu algoritma simetri dan asimetri (*public key algorithm*). Tujuan penulisan skripsi ini adalah untuk menjelaskan salah satu jenis *public key algorithm*, yaitu algoritma ElGamal ECC (*ElGamal Elliptic Curve Cryptography*).

Metode yang digunakan dalam penulisan skripsi ini adalah studi literatur dan implementasi program. Melalui studi literatur, dipelajari teori-teori yang berhubungan dengan kriptografi kurva *elliptic*, khususnya ElGamal ECC. Kemudian membuat program implementasinya.

Kekuatan ElGamal ECC tergantung pada panjang kunci yang digunakan dalam proses enkripsi dan dekripsi serta pemilihan parameter-parameter domainnya. Parameter-parameter tersebut dipilih sehingga diperoleh order *basic point* yang terbesar. Algoritma ElGamal ECC membutuhkan waktu yang lebih lama dibandingkan dengan *public key algorithm* yang lain, terutama operasi perkalian skalar kurva *elliptic* dan representasi *plaintext* menjadi titik. Tetapi memiliki tingkat keamanan yang tinggi dengan panjang kunci terpendek.

ABSTRACT

Wan Khudri, 2005. ENCRYPTION AND DECRYPTION DATA USING ElGamal ECC ALGORITHM. Faculty of Mathematics and Natural Sciences, Sebelas Maret University.

Cryptography is a science to keep information security, includes encryption and decryption. Encryption is a process to change plaintext into chipertext and decryption is a process to rechange chipertext into plaintext. The algorithm which is used in encryption and decryption called cryptographic algorithm. Based on the type of key, cryptographic algorithm is divided into two types, they are symmetry algorithm and asymmetry algorithm (public key algorithm).The purpose of this project is to explain one of the type of public key algorithm, that is ElGamal ECC algorithm.

The method of this writing project is literature study and implementation programme. Through literature study, learned the theories which is relevant to elliptic curve cryptography, especially ElGamal ECC. Then made the implementation programme.

The strenght of ElGamal ECC depend on the length of key which is used in encryption and decryption and also selection of the domain parameters. The parameters selected so that obtained the biggest of order basic point. ElGamal ECC algorihm needs longer time than the other public key algorithm, especially elliptic curve scalar multiplication and representation plaintext into point. But it has a high security level with the shortest key length.