International Conference on Instrumentation, Communication and Information Technology (ICICI) 2005
Proc., August 3rd -5th , 2005, Bandung, Indonesia

IMPLEMENTATION OF ElGamal ELLIPTIC CURVE CRYPTOGRAPHY USING MATLAB

Wan Khudri [1)], Sutanto [2)]

1) Jurusan Matematika, Universitas Sebelas Maret Surakarta
Jl. Ir. Sutami 36A, Kentingan, Surakarta 57126
e-mail: chudry81@yahoo.com or chudry@uns.ac.id

2) Jurusan Matematika, Universitas Sebelas Maret Surakarta
Jl. Ir. Sutami 36A, Kentingan, Surakarta 57126
e-mail: sutanto@uns.ac.id

ABSTRACT

ElGamal Elliptic Curve Cryptography(ECC) is a public key cryptography analogue of the ElGamal encryption schemes which is used Elliptic Curve Discrete Logarithm Problem (ECDLP). The software which is used to implement ElGamal ECC is MATLAB. This implementation consist of 3 main programmes, they are Key Generation, Encryption and Decryption ElGamal ECC.To reach the goal of the implementation, some *functions* which are able to construct the 3 main programmes are needed. Some *functions* are available in MATLAB and 31 *functions* are made by the writer himself. Those *functions* are classified into 3 categories, they are modular arithmetic *function* (7 *functions*), elliptic curve arithmetic *function* (5 *functions*) and ElGamal ECC *function* (19 *functions*).

The modular artihmetic *function* is used in addition operation, representation of NAF (Non Adjacent Form), multiplication operation, invers, division, power, and square root in modular arithmetic operation.

The elliptic curve arithmetic *function* is used in addition operation, elliptic curve equation, invers under addition, subtraction, and elliptic curve scalar multiplication.

The ElGamal *function* is used in biner-decimal conversion, decimal-biner conversion in '*n*' bit format, to find lower and upper bound of key length, to generate prime number, to generate coefficient of elliptic curve equation, to find the order of the elliptic group, to generate one elliptic curve point, to calculate the order of point, to generate base point and its order, elliptic curve domain parameters, to generate private key and public key, to represent plaintext into number, number into point, point into number, number into plaintext, encryption of ElGamal ECC for one point, and decryption of ElGamal ECC for one chipertext of point.

Key Words: ElGamal, elliptic curve, cryptography, field, public key