ISSN: 1391-8796
Proceedings of 8th Ruhuna International Science & Technology Conference
University of Ruhuna, Matara, Sri Lanka
February 17, 2021

A Modified Public Key Cryptosystem Based on the ELGAMAL Algorithm

Athurugiriya K.A.P.S.[1], Ranasinghe P.G.R.S.[1]

[1]*Department of Mathematics, Faculty of Science, University of Peradeniya, Peradeniya, Sri Lanka*

The ElGamal cryptosystem was introduced by Taher ElGamal in 1985. It is one of the most widely used public key cryptosystems and a probabilistic algorithm that was developed based on the Diffie-Hellman key exchange protocol. Unlike the Diffie-Hellman algorithm, this is a complete encryption-decryption system that depends on the discrete logarithm problem. Its security is based on the difficulty of finding the discrete logarithm modulo a large prime. We have introduced a generalized ElGamal algorithm using the Euler phi-function of the plaintext and the prime factorization of the plaintext. The algorithm is designed under the three primary steps of key generation, encryption, and decryption. The encryption process is improved in the sense that it depends on the Euler phi-function of the plaintext and the prime factorization of the plaintext. Modular exponentiation is taken twice during the encryption process, one with the multiplication of the Euler-phi function of the plaintext and the number of distinct prime factors of the plaintext with respect to the chosen prime number modulus and then with the secret encryption key. The key generation and the decryption process for the new system is similar to that of the standard ElGamal cryptosystem. The security of the system depends on the discrete logarithm problem which is known to be computationally hard. The proposed system preserves security against the Chosen Plaintext Attack (CPA).

Key words: *ElGamal Cryptosystem, Diffie-Hellman Key Exchange, Discrete Logarithm Problem, Euler Phi-Function, Chosen Plaintext Attack*

*Corresponding author: rajithamath@sci.pdn.ac.lk