ISSN: 1391-8796
Proceedings of 9th Ruhuna International Science & Technology Conference
University of Ruhuna, Matara, Sri Lanka
January 19, 2022

An improved public key cryptosystem based on ElGamal algorithm

Athurugiriya K.A.P.S. and Ranasinghe P.G.R.S.*
Department of Mathematics, University of Peradeniya, Peradeniya, Sri Lanka.

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It not only protects data from alteration, but also can be used for user authentication. Over the years, the original cryptographic schemes have been altered in order to achieve a higher level of security and efficiency. There are two main cryptosystems, symmetric and asymmetric depending on the key distribution properties. Public key cryptography or asymmetric cryptography is a scheme that uses pair of private keys and public keys. The generation of such key pairs depends on cryptographic algorithms which are based on certain mathematical techniques. ElGamal cryptosystem is an asymmetric cryptographic scheme which was introduced by Taher ElGamal in 1985. This algorithm was developed based on the Diffie-Hellman key exchange protocol. We have proposed a variant of the ElGamal scheme using two random integers instead of using one integer as used in the standard ElGamal cryptographic scheme. Then the new scheme becomes more intricate and challenging to decipher. This scheme is designed under three primary steps of key generation, encryption, and decryption. The key generation and encryption processes are improved due to the addition of one more random integer. The security of the system depends on the discrete logarithm problem which is known to be computationally hard.

Keywords: Discrete logarithm problem, ElGamal cryptosystem, Key generation, Encryption, Decryption

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