A GENERALIZED ELLIPTIC CURVE ELGAMAL CRYPTOSYSTEM

K.A.P.S. Athurugiriya, A.P. Madhushani and P.G.R.S. Ranasinghe*

Department of Mathematics, Faculty of Science, University of Peradeniya, Peradeniya, Sri Lanka
**rajithamath@sci.pdn.ac.lk*

Over the years, Elliptic Curves have been an active area of research. Around the mid-1980s, Koblitz, Lenstra Jr., and Miller independently developed the theory of Elliptic Curve cryptosystems whose significance is apparent from the statement made by the latter: "It is my intent to show that elliptic curves have a rich enough arithmetic structure so that they will provide a fertile ground for planting the seeds of cryptography". To withstand cryptanalysis over faster computers that also have higher processing capacities, classical cryptosystems have been forced to use larger keys for a secured communication. Thus, the future of Cryptography is most likely to be based on Elliptic Curve Cryptography (ECC), which provides an equivalent or higher security with smaller keys compared to that of the well-known cryptosystems. The heart of ECC lies within the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is believed to be computationally infeasible and hence, provides a higher level of security for Elliptic Curve cryptosystems. Elliptic Curve Diffie-Hellman and Elliptic Curve ElGamal algorithms are couple of renowned members of the family of ECC. We have introduced a Generalized ElGamal algorithm that uses the prime factorization of the plaintext and is proven to be secure against the Chosen Plaintext Attack. The Elliptic Curve version of our Generalized ElGamal algorithm also follows the prime factorization. If the plaintext is the power of a single prime, the proposed scheme is similar to the Elliptic Curve ElGamal cryptosystem. The security of the new method is guaranteed by the ECDLP.

Keywords: Chosen plaintext attack, ElGamal cryptosystem, Elliptic curves, Elliptic curve discrete logarithm problem