World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:13, No:05, 2019

An Attack on the Lucas Based El-Gamal Cryptosystem in the Elliptic Curve Group Over Finite Field Using Greater Common Divisor

Authors : Lee Feng Koo, Tze Jin Wong, Pang Hung Yiu, Nik Mohd Asri Nik Long

Abstract : Greater common divisor (GCD) attack is an attack that relies on the polynomial structure of the cryptosystem. This attack required two plaintexts differ from a fixed number and encrypted under same modulus. This paper reports a security reaction of Lucas Based El-Gamal Cryptosystem in the Elliptic Curve group over finite field under GCD attack. Lucas Based El-Gamal Cryptosystem in the Elliptic Curve group over finite field was exposed mathematically to the GCD attack using GCD and Dickson polynomial. The result shows that the cryptanalyst is able to get the plaintext without decryption by using GCD attack. Thus, the study concluded that it is highly perilous when two plaintexts have a slight difference from a fixed number in the same Elliptic curve group over finite field.

Keywords : decryption, encryption, elliptic curve, greater common divisor
Conference Title : ICAMCS 2019 : International Conference on Applied Mathematics and Computer Sciences
Conference Location : Amsterdam, Netherlands
Conference Dates : May 14-15, 2019