Common modulus attack against Lucas based El-Gamal Cryptosystem in the elliptic curve group over finite field

ABSTRACT

Common modulus attack is one of the various homomorphic attacks based on homomorphism nature of cryptosystems. This type of attack requires a plaintext encrypted under same modulus while two encryption keys are relatively prime to each other. In this paper, an investigation was carried out to evaluate the nature of a homomorphic attack on the Lucas based El-Gamal Cryptosystem in the elliptic curve group over finite field. The attack can be proven by using extend Euclidean algorithm together with composite and reverse functions of Lucas and Fibonacci sequences. Results showed that common modulus attack can be used to obtain the original plaintexts. Thus, it is dangerous to send a plaintext to two different users using same modulus. Sender must use different modulus to communicate with two different users.

Keyword: Decryption; Encryption; Fibonacci Sequence; Lucas Sequence; Modulus