Security analysis of Lucas based El-Gamal Cryptosystem in the elliptic curve group over finite field using two types of GMITM attacks

ABSTRACT

The success of Garbage-man-in-the-middle (GMITM) attack relies on the possibility to access to the ”bin” of recipient in the cryptosystem. It is capable to recover the original plaintext by granting an entry to the ”bin”. There are basically two types of GMITM attacks, a polynomial attack and a homomorphic attacks. In this paper, an investigation was carried out to evaluate the polynomial structure of cryptosystem and the nature of a homomorphic attack on cryptosystem. The results show that the cryptanalyst could obtain the plaintext without knowing the secret number, a, b and R.

Keyword: Bin; Decryption; Elliptic curve; Encryption; Lucas sequence