Cryptographic attack on LUC-type cryptosystems using GMITM (Type 1)

ABSTRACT

Garbage-man-in-the-middle (type 1) attack is an attack exploit the polynomial structure of LUC-type cryptosystems and depends on the possibility to get the faulty plaintext in the bin of the receiver. This paper reports an investigation for LUC-type cryptosystems under garbage-man-in-the middle (type 1) attack. Among all LUC-type cryptosystems, LUC, LUC3, and LUC4, 6 are selected to analyze their security. Results show that the attack fully success into the selected LUC-type cryptosystems under certain conditions.

Keyword: Lucas sequence; Encryption; Decryption; Plaintext; Ciphertext; Relatively prime; Bin