On the common modulus attack into the LUC4,6 cryptosystem

ABSTRACT

The LUC4,6 cryptosystem is a system analogy with RSA cryptosystem and extended from LUC and LUC3 cryptosystems. The process of encryption and decryption are derived from the fourth order linear recurrence sequence and based on Lucas function. This paper reports an investigation into the common modulus attack on the LUC4,6 cryptosystem. In general, the common modulus attack will be succeeded if the sender sends the plaintext to two users used same RSA-modulus and both of encryption keys of them are relatively prime to each other. However, based on the characteristics of high order Lucas sequence, the LUC4,6 cryptosystem is unattackable.

Keyword: Common modulus; Linear recurrence sequence; Lucas function