Computation of private key for LUC cryptosystem

ABSTRACT

LUC cryptosystem is a public key cryptosystem based on Lucas functions. The encryption of this cryptosystem is relatively easy since we have the knowledge of public key e, two primes p and q and also the message M. Meanwhile, decryption process is difficult without the knowledge of private key d. In this paper, we are presenting a technique that can be used to compute private key for LUC cryptosystem. It is based on the existing number theory techniques. The computation of private key is possible because we know values of two primes p, q and ciphertext C. The size of two primes is important that determined the size of private key.

Keyword: LUC cryptosystem; Encryption; Decryption; Private key