Computation of cryptosystem based on Lucas functions using addition chain

ABSTRACT

Cryptosystem based on Lucas Functions is known as LUC Cryptosystem. Lucas Functions are the special form of second-order linear recurrence relation using a large public integer as modulus. In this paper, an efficient computation algorithm for LUC Cryptosystem is developed. It is based on Addition Chain. The computation time for existing and new algorithms will be recorded. Smaller computation time means the algorithm is efficient than the other. New technique shows a smaller computation time compared to the existing algorithm. It also increases the efficiency of computation. At the same time, it also reduces some iteration that is involved in LUC Cryptosystem computation.

Keyword: Computation algorithm; Addition chain; Lucas functions