A method to decrease computation time for fourth order Lucas sequence

ABSTRACT

The fourth order Lucas sequence is a linear recurrence relation related to quartic polynomial and based on Lucas function. This sequence had been used to develop the LUC4,6 cryptosystem. As we know, the efficiency is one of the crucial parts of the cryptosystem and it is depended on computation time for Lucas sequence which is used to develop the process encryption and decryption in the LUC4.6 cryptosystem. In this paper, a method will be proposed to decrease the computation time for fourth order Lucas sequence. This method omits some terms of the sequence to decrease the computation time. Thus, if the LUC4,6 cryptosystem is using this method to compute the plaintexts and cipher texts, then the computation time had been decreased.

Keyword: Computation time; Lucas sequence; Terms of sequence