Cryptographic attack on Lucas based cryptosystems using chinese remainder theorem

ABSTRACT

Lenstra's attack uses Chinese remainder theorem as a tool and requires a faulty signature to be successful. This paper reports on the security responses of fourth and sixth order Lucas based (LUC4,6) cryptosystem under the Lenstra's attack as compared to the other two Lucas based cryptosystems such as LUC and LUC3 cryptosystems. All the Lucas based cryptosystems were exposed mathematically to the Lenstra's attack using Chinese Remainder Theorem and Dickson polynomial. Result shows that the possibility for successful Lenstra's attack is less against LUC4,6 cryptosystem than LUC3 and LUC cryptosystems. Current study concludes that LUC4,6 cryptosystem is more secure than LUC and LUC3 cryptosystems in sustaining against Lenstra's attack.

Keyword: Lucas sequence; Dickson Polynomial; Faulty signature; Corresponding signature; Congruence