World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:13, No:05, 2019

Cryptographic Attack on Lucas Based Cryptosystems Using Chinese Remainder Theorem

Authors : Tze Jin Wong, Lee Feng Koo, Pang Hung Yiu

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 (LUC_{4,6}) 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 LUC_{4,6} cryptosystem than LUC₃ and LUC cryptosystems. Current study concludes that LUC_{4,6} cryptosystem is more secure than LUC and LUC₃ cryptosystems in sustaining against Lenstra’s attack.

Keywords : Lucas sequence, Dickson polynomial, faulty signature, corresponding signature, congruence
Conference Title : ICAMCS 2019 : International Conference on Applied Mathematics and Computer Sciences
Conference Location : Amsterdam, Netherlands
Conference Dates : May 14-15, 2019