On the wiener's attack into lucas based El-gamal cryptosystem in the elliptic curve over finite field

ABSTRACT

This paper reports a security analysis on the Lucas Based El-Gamal Cryptosystem in the Elliptic Curve Over Finite Field. Wiener's Attack was selected to analyze the cryptosystem under a bad implementation practice. Result showed that the cryptosystem was weak if the chosen keys were too small among those in the order of group G.

Keyword: Encryption; Decryption; Elliptic curve; Lucas sequence