Lucas based el-gamal cryptosystem in the elliptic curve group over finite field under lenstras attack

ABSTRCT

This paper reports on a Lenstra's attack against the Lucas based El-Gamal Cryptosystem in the elliptic curve group over finite field. Lenstra's attack is an attack to recover the secret factor of the order of elliptic curve group from a faulty signature. Results show that the success of the Lenstra's attack depend on cryptographic algorithm implementation practice rather than the weakness of the cryptosystem itself

Keyword: Faulty signature; Lucas sequence; Elliptic curve; Encryption; Decryption.