

Abstract

Cryptography method that use for encryption voice on GSM Mobile communication system use cryptography A5 algorithm. A5 algorithm is kind symmetry algorithm where key is use for encryption and decryption process is same. A5 algorithm is divided into A5/1,A5/2, and the new version is A5/3.

This final project have objective to simulate and analysis capability algorithm cryptography of A5/2, with method analysis random distribution in output, time process and performance, and avalanche effect. For avalanche effect result, will be compare with algoritma A5 with ECC (Elliptic Curve Cryptography) result.

Keywords : *Cryptography, GSM (Global System for Mobile Communications, A5, A5/2, A5 with ECC, Avalanche effect.*

Hypothesis: Security system at GSM (Global System for Mobile Communications) use ciphering A5/2 algorithm weak version of A5 algorithm, because internal structure A5/2 algorithm not to complex, and A5 with ECC is algorithm to overcome the weakness from A5/2.