Abstract

Cryptography is an art and science for save data. GSM (Global System for Mobile Communications) is mobile communication system that have subscriber increase exponentially, so that to keep from fraud between BS (Base Station) and MS (Mobile Station) from people or institution which not subscriber legal, so need ciphering voice.

Cryptography 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 as strong version and A5/2 as weak version to protect real time voice at air between MS and BS on GSM (Global System for Mobile Communication). A5/1 algorithm is input function key (K_c) and frame number (F_n) with 114 bit stream output. A5/1 algorithm contains 3 LFSRs with clock control.

This final project have objective to proof and analysis capability both algorithm cryptography system, with method analysis structure A5/1 algorithm, random distribution at output, avalanche effect, process performance, strong ability from few attack and analysis BER at system

Key word: *Cryptography, GSM (Global System for Mobile Communications), MS (Mobile Station, BTS (Base Transmission Station), A5, stream cipher, LFSR (Linear Feedback Shift Register), A5/1, A5/2.*

Hypothesis: *Security system at GSM (Global System for Mobile Communications) use ciphering A5/1 algorithm give capability security is better than A5/2 algorithm, because internal structure A5/1 algorithm more complex than A5/2 algorithm.*