Abstract

A5/3 algorithm is a new version of A5 algorithm. It is used to encrypt voice and data from mobile phone to Base Transceiver Station (BTS). This algorithm based on KASUMI algorithm, that produces 64 bit output from 64 bit input with 128 bit key. Output from this algorithm are two blocks contain each 114 bit. That blocks is used for encrypt/decrypt on uplink and downlink. Application of algorithm A5/3 is made as simulator to simulate that algorithm. Avalanche effect, process time, and changing of file size are parameter to measure strength of algorithm. Based on this experiments, result of avalanche effect is 51.053% for case that flipping single bit of key with same plaintext. The other hand, avalanche effect for the case that flipping one bit plaintext with same key is 0.877%. The process time increase as same as increasing of file size. So, the large file size need much time to process. The output file size as same as input file size. Therefore, it same as behavior of A5/3 algorithm that a stream cipher.

Keywords: A5/3, encrypt, decrypt, avalanche effect, time process, file size