ABSTRACT

International standard of 3G security mobile communication systems is ruled on UMTS (Universal Mobile Telecommunication System). Security system on the network has a lot cryptography algorithm that used. Cryptography algorithm that used in 3G technology are f8 and f9 algorithm, it is used to protect network security system between UE (User Equipment) and RNC (Radio Network Controller). These algorithms are made based on A5/3 (Kasumi) algorithm, which is symmetric algorithm with encryption and decryption has 64-bit cipher block and 128-bit keys.

In this final project, focus on design and implementation A5/3 (Kasumi) algorithm using DSP Card TMS320VC33. TMS320VC33 is DSP (Digital Signal Processing) card which has 150 MFLOPS (Million Floating Point Operations per Seconds) velocity's operation or equal with 75 MIPS (Million Instruction per Second), so it can do real time digital signal processing. Design implementation doing by make program based on the cryptography algorithm using assembly language, then implemented it into TMS320VC33. The performance of encryption output is analyzed using time processing, avalanche effect, and brute force attack.

From the test result conclude that system can be realized with time process 2,97x 10^{-2} ms, it is calculated from duty cycle. The value of avalanche effect based on 1 bit key changing reaches 48,88%, for 1 bit change of plaintext is 49,66 %, and for 1 bit change of ciphertext is 50,15%. Time to do brute force attack is $1{,}60 \ x \ 10^{26}$ years.

Keywords: f8 and f9 algorithm, A5/3 (Kasumi) algorithm, *DSP Card TMS*, *avalanche effect*, *time processing brute force attack*