

ABSTRACT

. UMTS (Universal Mobile Telecommunication System) is a third generation wireless communication system which is the increasing of GSM (Global System for Mobile Communication). Because of the increase in cellular technology (wireless), the safety system get more attention to avoid the information robbing by the others side or groups who are not responsible.

Safety system of UMTS link use f8 and f9 cryptography algorithm to keep the confidentiality and integrity of data between User Equipment (UE) and Radio Network Controller (RNC). f8 algorithm is algorithm for encryption and decryption process to protect data confidentiality and f9 algorithm is algorithm to produce code attached to data for protect integrity. f8 and f9 algorithm is made according to KASUMI block cipher algorithm, a kind of simetry algorithm, where the key which is used to encryption and decription proces is 64-bit input and the 128-bit key will produce 64-bit output. This thesis specially discuss about cryptography f8 and f9 algorithm simulation using Matlab 2007a. It also try to prove the ability of f8 and f9 algorithm system by analizing time and performance process, then analizing random distribution level or the changing of the bit and *avalanche effect* from f8 algorithm. And measure ability the f8 and f9 algorithm of *brute force attack*.

From the result of some test, it can be concluded that the f8 algorithm input and output bit changging for text =53,5125%, voice=51,254%, dan picture=49,81162%. Time and Performance process for f8 and f9 is almost the same. *Avalanche effect* value of f8 algorithm for one bit key changing is 50,23202% while for one bit *plaintext* or *ciphertext* is about 3,125%. Otherwise, the delay to do *brute forced attack* for f8 and f9 algorithm is $1,618 \times 10^{40}$ years.

Keyword: UMTS, f8 and f9 Algorithm, KASUMI, brute force attack dan avalanche effect