ABSTRACT

As the time goes by, the need of security over transmitted data becomes even greater. It is caused by the sensitivity of the information that is being exchanged by the users. In communication system nowadays, *Wifi Protected Access* 2 (WPA2) is implemented in Wi-Fi connection, using AES as its encryption method. AES is a symmetric algorithm, which means that two users need to use the same key. It's impractical because for the encryption method to be secured, the key needs to be sent through a very secured channel. In previous research by Rohan Rayarikar, Sanket Upadhyay, and Priyanka Pimpale, an encryption method has been implemented using *Advanced Encryption Standards (AES)* to encrypt data that are transmitted using SMS technology. Another problem that occurs apart from security problems in mobile telecommunication system is resolving the *multipath fading* in propagation channel, especially *frequency-selective fading.*

To solve the security problems of data information, *Elliptic Curve Cryptography* encryption method is implemented in this research as an *end to end* algorithm to increase data security. To solve the *frequency-selective fading* problems in propagation channel, this research also implements *Orthogonal Frequency Division Multiplexing* (OFDM) in its simulation. 16-QAM and QPSK are the modulation schemes that are used in this research, along with the addition of *Additive White Gaussian Noise* (AWGN) and *Rayleigh Fading* in the propagation channel. The parameters used and compared in this research are *Bit Error Rate* (BER) and the result of decrypted data when being compared with the original data for the value of Eb/No from 0 dB to 20 dB.

The encrypted data have no similarity in terms of characters with the original data. Performance simulation shows that the ECC encryption gives correlation for a value of 0.018, entropy with value of 7.9877, sensitive with key changes, and need a lot of time to calculate the key using Brute Force Attack. Data received after decryption proses have 6 characters errors in total compared to original data in Eb/No with value of 8 dB, and have 1 character errors in total compared to original data in Eb/No with value of 20 dB. The system using ECC encryption method has higher BER results than system without ECC encryption method, with 0.0014 BER difference in Eb/No with value of 20 dB. The system using QPSK modulation scheme has lower BER than system using 16-QAM modulation scheme, with 0.0072 BER difference in Eb/No with value of 20 dB.

Keywords : Cryptography, ECC, OFDM