ABSTRAK

Seiring dengan berjalannya waktu, kebutuhan akan keamanan informasi pada data yang ditransmisikan menjadi semakin besar. Hal ini disebabkan karena data yang dikirimkan antara dua *user* yang berkomunikasi terkadang merupakan data yang sifatnya sensitif dan rahasia. Pada sistem komunikasi saat ini, terutama pada jaringan Wi-Fi, telah terdapat suatu metode enkripsi *Wifi Protected Access 2* (WPA2), yang mengimplementasikan AES pada enkripsinya. AES merupakan algoritma kriptografi simetris, sehingga pengirim dan penerima harus menggunakan kunci yang sama. Hal ini tentu akan menyusahkan karena kunci yang digunakan harus dikirim menggunakan jaringan komunikasi yang benar-benar aman. Pada penelitian sebelumnya yang dilakukan Rohan Rayarikar, Sanket Upadhyay, dan Priyanka Pimpale, telah diterapkan suatu metode enkripsi menggunakan algoritma *Advanced Encryption Standards* (AES) untuk mengenkripsi data yang dikirimkan menggunakan layanan SMS. Selain dari masalah keamanan, kendala yang banyak dihadapi pada sistem komunikasi *mobile* saat ini adalah bagaimana mengatasi propagasi yang bersifat *multipath*, sehingga menyebabkan terjadinya *multipath fading*, khususnya *frequency-selective fading*.

Untuk mengatasi permasalahan pada keamanan informasi data, pada tugas akhir ini ditawarkan penggunaan algoritma *Elliptic Curve Cryptography* (ECC) sebagai algoritma untuk meningkatkan keamanan informasi pada data, secara *end to end*. Selain itu, pada simulasi tugas akhir ini digunakan skema transmisi OFDM untuk mengatasi kanal yang bersifat *frequency-selective fading*. Pada simulasi ini juga digunakan dua tipe modulasi, yaitu *16-Quadrature Amplitude Modulation* (16-QAM) dan *Quadrature Phase Shift Keying* (QPSK), serta penambahan *Additive White Gaussian Noise* (AWGN) dan *Rayleigh Fading* yang bersifat *frequency-selective* pada kanal transmisi. Parameter yang digunakan sebagai perbandingan dalam analisis hasil simulasi adalah *Bit Error Rate* (BER), dan hasil *ciphertext* dan *plaintext* pada sisi pengirim dan penerima untuk nilai Eb/No berkisar antara 0-20 dB.

Data asli setelah proses enkripsi mengalami perubahan secara keseluruhan. Simulasi performansi memberikan hasil *correlation sebesar* 0.0064, nilai entropy sebesar 7.4186, sensitif terhadap perubahan kunci, dan membutuhkan waktu yang sangat lama untuk mencari nilai kunci menggunakan teknik *Brute Force Attack* pada nilai kunci yang tinggi. Data yang diterima setelah proses dekripsi memiliki 24 buah karakter yang berubah dari data asli pada nilai Eb/No 8 dB, dan memiliki 1 buah karakter yang berubah pada nilai Eb/No 20 dB. Nilai BER sistem yang memakai metode enkripsi ECC sedikit lebih besar dari sistem yang tidak memakai metode enkripsi ECC, dengan perbedaan nilai BER sebesar 0.0014 pada Eb/No 20 dB. Nilai BER sistem yang memakai modulator QPSK lebih kecil dari sistem yang memakai modulator 16-QAM, dengan perbedaan nilai BER sebesar 0.0072 pada Eb/No 20 dB.

Kata Kunci : *Kriptografi, ECC, OFDM*