

ABSTRAK

Pengiriman atau pertukaran data adalah hal yang sering terjadi dalam dunia teknologi informasi. Untuk menjaga keamanan data, dapat dilakukan dengan menggunakan teknik kriptografi. salah satunya adalah Teknik kriptografi *AES-Turbo Code*. Penelitian ini mengusulkan *new joint Error-Correction* dan skema enkripsi berbasis turbo code, yang dapat disebut sebagai enkripsi berbasis turbo. Skema ini seharusnya memiliki kemampuan *Error-Correction* serta keamanan yang tinggi. untuk mengenkripsi informasi dari *Turbo Code* terdapat dua Langkah : Langkah pertama yaitu interleaver dari *Turbo Code* di tingkatkan, dimana dapat di kontrol oleh pengontrol kunci rahasia. Sedangkan pada langkah kedua interleaver lainnya di tambahkan ke output pertama dari turbo enkoder, dimana juga di kontrol oleh pengontrol kunci rahasia. simulasi menunjukkan pada skema ini memiliki kinerja yang baik dalam keamanan dan kemampuan *Error-Correction*. Penelitian ini hanya membuat simulasi Teknik Kriptografi *AES-Turbo Code* dengan pengontrol kunci rahasia dalam enkripsi dan dekripsi menggunakan data soal ujian online CPNS. Semakin panjang data text inputan maka semakin lama waktu yang dibutuhkan untuk enkripsi dan dekripsi. *Performa Bit Error Rate (BER)* dengan Noise AWGN dapat berjalan baik pada SNR 15dB-25dB. Variasi panjang kunci AES 256-bit lebih baik dari 128-bit dengan perbedaan *Avalanche Effect* sebesar 43,41805%.

Kata Kunci : *AES, Turbo code, AES-Turbo, Secret Key Controller, Kunci Rahasia, Interleaver, Soal Ujian Online, Enkripsi, Dekripsi*