

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pengiriman atau pertukaran data adalah hal yang sering terjadi dalam dunia teknologi informasi[1]. Enkripsi informasi berdasarkan Error-Correction adalah ide yang menarik untuk komunikasi secara rahasia karena dua alasan berikut: 1.) kode Error-Correcting menghasilkan paritas bits dengan mengubah urutan struktur informasi aljabar, yang mirip dengan enkripsi informasi. Sehingga begitu mudah untuk mengubah kode Error-Correction menjadi skema enkripsi. 2.) informasi yang dienkripsi dapat menolak noise, untuk skema enkripsi yang didasarkan pada kode Error-Correction[6].

Ada beberapa penelitian tentang enkripsi error correction, tetapi kebanyakan menggunakan dua langkah untuk enkripsi sebuah informasi dan error-correction. The National Scientific Foundation (NSF) dari USA membentuk sebuah grup untuk mempelajari tentang menyatukan enkripsi dan error-correction bersama. Mereka hanya memberikan sebuah laporan dan menekankan tentang pentingnya dari enkripsi error-correction, tetapi mereka tidak mengusulkan skema pengkodean secara rinci [13]. *Glignoski et al* mengusulkan skema penggabungan error-correction dan enkripsi, akan tetapi kode error-correction dalam skema ini didasarkan pada hard decision, oleh karena itu kemampuan error correction pada skema ini terbatas. Karena kinerja error-correction dari turbo code sangat baik dan turbo code digunakan secara luas, menguntungkan untuk merancang algoritma enkripsi menggunakan turbo code.

Skema informasi enkripsi berbasis turbo code memiliki tingkat keamanan dan error-correction yang baik. Skema pada turbo code menambahkan enkripsi (atau interleaver) sebelum turbo enkoder. Enkripsi ini menyajikan informasi enkoder dalam beberapa turbo frame, sehingga membutuhkan lebih lama waktu delay ketika decode.

Pada penelitian ini mengusulkan metode enkripsi baru menggunakan turbo code. Pada metode ini interleaver enkoder dan dekoder dikendalikan oleh pengontrol kunci rahasia. Selanjutnya interleaver luar di adopsi sebelum turbo

enkoding. Dalam skema ini informasi dienkripsi saat turbo encoding, sehingga dibutuhkan waktu yang lebih cepat ketika enkripsi sebuah informasi. Kedua interleaver ini memastikan keamanan yang tinggi dari skema enkripsi.

Dari hal-hal yang disebutkan diatas, maka penulis membuat Simulasi Pengamanan Data Teks Rahasia Menggunakan Metode Kriptografi AES-Turbo Code Dengan Pengontrol Kunci Rahasia dengan menggunakan latar belakang yaitu unsur-unsur yang telah disebutkan di atas.

1.1. Perumusan Permasalahan

Berdasarkan dari latar belakang diatas, dapat mendefinisikan sebuah masalah yang di-kaji dalam penelitian ini sebagai berikut :

1.2.1 Masalah

Metode kriptografi enkripsi dan dekripsi pada data teks yang telah digunakan sebelumnya kurang akurat dan efisien untuk mendapatkan error-correction yang tinggi.

1.2.2 Metode Yang Diusulkan

Pengamanan Data Teks Kriptografi AES-Turbocode Dengan Pengontrol Kunci Rahasia (Secret Key Controller).

1.2.3 Pertanyaan Penelitian

1. Seberapa efisiensi algoritma kriptografi AES-Turbo code dan pengontrol kunci rahasia dengan variasi kunci rahasia pada data text ujian online yang di perlukan untuk enkripsi dan dekripsi berdasarkan parameter waktu (waktu eksekusi data) ?
2. Seberapa efektifitas performa kriptografi AES-Turbo code dan pengontrol kunci rahasia dengan variasi kunci rahasia pada data text ujian online yang di perlukan untuk enkripsi dan dekripsi berdasarkan *Bit Error Rate* (BER) ?
3. Bagaimana perbandingan efisiensi dan efektifitas kriptografi AES-Turbo code dan pengontrol kunci rahasia dengan variasi kunci rahasia yang berbeda pada data text ujian online berdasarkan *Avalanche Effect* ?

1.3. Tujuan dan Manfaat

Adapun Tujuan dan manfaat yang dapat diambil dari permasalahan diatas antara lain:

1.3.1 Tujuan

Tujuan Berdasarkan perumusan masalah di atas, maka tujuan yang ingin dicapai dalam penelitian yaitu,

1. Membandingkan efisiensi kombinasi algoritma kriptografi AES-Turbo dan pengontrol kunci rahasia berdasarkan parameter waktu yang diperlukan untuk enkripsi & dekripsi (waktu eksekusi data).
2. Mengetahui dan menganalisa performa kombinasi kriptografi AES-Turbo code dan pengontrol kunci rahasia dengan uji coba *Bit Error Rate* (BER) dan persentase data kembali.
3. Mengetahui dan menganalisa efisiensi dan efektifitas performa kombinasi kriptografi AES-Turbo code dan pengontrol kunci rahasia dengan uji coba *avalanche effect*.

1.3.2 Manfaat

Manfaat yang dapat diambil dari penelitian ini adalah dapat menganalisa kinerja dari kombinasi AES-Turbo dengan Secret Key Controller (pengontrol Kunci Rahasia) berdasarkan parameter waktu yang diperlukan untuk enkripsi& dekripsi (waktu eksekusi data), *avalanche effects* dan BER (*Bit ErrorRate*).

1.4 Batasan Masalah

1. Data yang di proses berupa inputan soal ujian online CPNS. Dataset ujian online yang diambil dari dataset (<https://www.awambicara.id/2018/01/contoh-soal-tkd-cpns-dan-pembahasannya.html>).
2. Panjang kunci AES yang digunakan 128-bit, 192-bit, dan 256-bit.
3. Turbo Code menggunakan algoritma Maximum posteriori (MAP).
4. Kanal berderau (noise) yang digunakan yaitu kanal AWGN dengan kondisi SNR 5.0 dB hingga 15.0 dB sebagai parameter pembangkit noise (AWGN).
5. Parameter sistem kriptografi ditinjau dari *avalanche effect*, Waktu enkripsi/deskripsi dan BER (*Bit Error Rate*).