

BAB I

PENDAHULUAN

1.1. Latar Belakang

Pengiriman atau pertukaran data adalah hal yang sering terjadi dalam dunia teknologi informasi[1]. Perkembangan yang pesat dalam proses pengiriman atau pertukaran data membawa dampak yang besar, yaitu masalah keamanan data yang dikirim[2]. Data yang dikirim kadang sering berisi data informasi yang penting bahkan sangat rahasia dan harus dijaga keamanannya. Pengiriman data yang dilakukan melalui layanan komunikasi dunia maya, biasanya terjadi ancaman kejahatan yang sangat banyak. Dengan adanya ancaman kejahatan seperti *interception* (penyadapan), akibatnya data bisa jatuh pada orang yang tidak berhak bahkan data akan disalahgunakan oleh pihak yang tidak berwenang[1]. Selain itu dalam komunikasi data terkadang terdapat gangguan berupa derau (*noise*)[3] sehingga data yang dikirim rentan terjadi kerusakan. Kerusakan data disini yaitu berupa pengurangan atau penambahan bit bit pada data yang menyebabkan data tersebut tidak seperti pada saat sebelum dikirim.

Untuk mengatasi beberapa masalah di atas dapat dilakukan dengan menerapkan kombinasi antara teknik kriptografi dan FEC (*Forward Error Correction*). Kombinasi yang digunakan adalah AES (*Advanced Encryption Standard*) Sebagai teknik kriptografi dan Turbo Code sebagai FEC (*Forward Error Correction*). AES merupakan enkripsi yang menggunakan kunci simetris. Standar ini terdiri atas 3 blok cipher, yaitu AES-128, AES-192 dan AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Masing-masing cipher memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit [4]. Sedangkan *Turbo Code* merupakan salah satu metode FEC (*Forward Error Correction*). FEC adalah metode yang mampu mengoreksi *error* dari informasi yang ditransmisikan. Koreksi terhadap *error* dilakukan dengan menggunakan teknik coding sebelum data dikirimkan dan sebelum data diterima[5].

Metode kombinasi AES dan Turbo Code sudah pernah diteliti sebelumnya yakni penelitian dari Hakan CAM, Volkan OZDURAN dan Osman N. UCAN yang di beri nama AES-Turbo. Pada penelitian tersebut menjelaskan bahwa 2 teknik tersebut dapat dikombinasikan dengan cara meletakkan turbo enkoder didalam enkripsi AES pada



iterasi pertama setelah *SubBytes* dan meletakkan turbo dekodeur didalam dekripsi AES pada iterasi terakhir sebelum *SubBytes* sehingga proses tersebut tidak saling terpisah atau menjadi suatu kesatuan[6]. Kombinasi AES-Turbo menjadi lebih aman dikarenakan terdapat proses penambahan enkoder pada enkripsi. enkoder ini berfungsi selain sebagai *error correction* juga sebagai pengacakan bit-bit setelah *SubBytes*.

Pada penelitian ini, penulis menggunakan metode tersebut pada sisi enkripsi untuk menganalisa perbandingan kombinasi tersebut terhadap tiga variasi kunci AES dengan parameter uji yaitu waktu yang diperlukan untuk enkripsi & dekripsi (waktu eksekusi data), avalanche effects dan BER (Bit Error Rate).

1.2. Perumusan Masalah

Berdasarkan latar belakang masalah yang telah dipaparkan diatas, maka penulis merumuskan permasalahan pada penelitian ini sebagai berikut:

1. Bagaimana performa kombinasi AES - Turbo Code dengan tipe data text yang dilewatkan pada kanal ideal dan berderau (*noise*) dengan kondisi SNR 5 dB hingga 15 dB sebagai parameter pembangkit *noise* (awgn)?
2. Bagaimana perbandingan efisiensi dan efektifitas kombinasi algoritma kriptografi AES-Turbo terhadap tiga variasi kunci AES?

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 ini adalah sebagai berikut :

1. Mengetahui dan menganalisa performa kombinasi AES-Turbo dengan ujicoba Bit Error Rate dan presentase data kembali.
2. Membandingkan efisiensi dan efektifitas kombinasi algoritma kriptografi AES-Turbo berdasarkan ragam panjang kunci pada AES terhadap parameter waktu yang diperlukan untuk enkripsi & dekripsi (waktu eksekusi data), avalanche effects.



1.3.2. Manfaat

Manfaat yang dapat diambil dari penelitian ini adalah dapat menganalisa kinerja dari kombinasi AES-Turbo dengan tiga variasi kunci AES berdasarkan parameter waktu yang diperlukan untuk enkripsi & dekripsi (waktu eksekusi data), *avalanche effects* dan BER (*Bit Error Rate*).

1.4. Batasan Masalah

Batasan masalah dari penelitian ini antara lain:

1. Data yang diproses berupa text yang diinputkan (berupa soal ujian dan jawabannya sebanyak 1-3 halaman / text $\pm 2721-7826$ karakter).
2. Parameter sistem kriptografi ditinjau dari *avalanche effect*, waktu enkripsi/dekripsi(waktu eksekusi data) dan BER (*Bit Error Rate*).
3. Panjang kunci yang digunakan yaitu 128-bit, 192-bit dan 256-bit.
4. Parameter input turbo code yang digunakan yaitu: $g=[1\ 1\ 1;0\ 0\ 0]$, *code-rate*=1/2(puncture), iterasi dekoder=1, dan menggunakan dekoder Log-MAP.
5. Kanal berderau (*noise*) yang digunakan yaitu kanal awgn dengan kondisi SNR 5 dB hingga 15 dB sebagai parameter pembangkit *noise* (awgn).

1.5. Metodologi Penelitian

Secara garis besar tahapan metodologi penelitian yang digunakan dalam penelitian Tugas Akhir ini adalah sebagai berikut:

1. Studi Pustaka
Proses pengumpulan data dan informasi dengan mempelajari materi-materi tentang algoritma enkripsi AES dan *Turbo code*.
2. Perumusan Masalah
Pada tahap ini yang dikejakan adalah merumuskan masalah yang didapat, dan menentukan kebutuhan sistem yang tepat untuk mengatasinya.
3. Analisa dan Perancangan
Pada tahap ini proses analisa sistem dan mulai dilakukan perancangan *design* dari sistem yang akan digunakan.
4. Implementasi



Pada proses ini dilakukan pengimplementasian dan kombinasi antara metode Enkripsi data *AES* dan *Turbo code*.

5. Evaluasi
Pada tahapan ini adalah melakukan evaluasi terhadap sistem yang dibuat. Apa bila terjadi kekurangan maka akan dilakukan perbaikan.
6. Penulisan Laporan
Tahap ini merupakan tahap terakhir dari penyusunan tugas akhir. Pada tahap ini dilakukan penulisan laporan dari tugas akhir yang dikerjakan.

1.6. Sistematika Penulisan

Secara garis besar, Sistematika penulisan buku dalam Tugas Akhir ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang penelitian, perumusan masalah, tujuan, manfaat, batasan masalah, metode penelitian, serta sistematika penulisan dalam laporan tugas akhir ini.

BAB II : STUDI PUSTAKA

Bab ini membahas mengenai landasan teori-teori pokok yang digunakan dalam menyusun penelitian ini. Landasan teori yang dibahas meliputi teori umum dan teori khusus.

BAB III : PERANCANGAN SISTEM

Pada bab ini menjelaskan tentang rancangan sistem dan keseluruhan sistem yang dibuat beserta rancangan alur flowchart pada tiap-tiap proses pada sistem.

BAB IV : IMPLEMENTASI SISTEM

Pada bab ini menjelaskan tentang implementasi sistem berdasarkan rancangan pada BAB III. Dan menjelaskan hasil analisa dari sistem yang telah dibuat.

BAB V : PENUTUP

Pada bab penutup ini menjelaskan tentang kesimpulan dari hasil uji coba yang telah dilakukan serta saran yang menjadi masukan dalam pengembangan penelitian berikutnya.

