

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang permasalahan, rumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian, dan sistematika penulisan dalam penelitian ini.

1.1. Latar Belakang

Keamanan informasi merupakan sesuatu yang harus diperhatikan secara serius. Perkembangan teknologi informasi semakin memudahkan penggunaanya dalam berkomunikasi melalui berbagai media. Keamanan informasi dilakukan untuk melindungi informasi/data pribadi terhadap ancaman yang mungkin akan timbul melalui tindakan kejahatan komputer yang memanfaatkan celah dari keamanan untuk mengambil atau memanipulasi data. Terdapat berbagai metode yang bisa kita gunakan untuk melindungi keamanan data contohnya seperti menggunakan *password* dan enkripsi data.

Untuk menghindari pesan atau informasi yang dikirim tidak disalah gunakan oleh pihak yang tidak berkepentingan maka perlu dilakukan proses enkripsi pesan asli dan penyisipan pesan ke dalam suatu media. Salah satu bidang ilmu untuk menjaga keamanan informasi adalah kriptografi. Dengan kriptografi, informasi yang dianggap rahasia dapat disembunyikan dengan teknik penyandian, sehingga tidak bisa dimengerti oleh orang lain, selain pembuat dan penerima pesannya saja. Konsep kriptografi untuk menjaga kerahasiaan data adalah dengan cara menyamarkannya menjadi bentuk sandi-sandi yang tidak bisa dibaca. Pesan yang disandikan disebut *plaintext*, sedangkan pesan yang disamarkan disebut dengan *chipertext*. Proses penyamaran dari *plaintext* ke *chipertext* disebut enkripsi, sedangkan proses pengembalian *chipertext* menjadi *plaintext* disebut dengan dekripsi [1].

Banyak sekali jenis algoritma kriptografi, diantaranya adalah algoritma Rijndael yang sekarang ditetapkan menjadi *Advanced Encryption Standard* (AES). AES merupakan salah satu jenis teknik kriptografi yang ditetapkan oleh lembaga standar Amerika Serikat bernama NIST (*Nasional Institute of Standards and Technology*). Pada tahun 2001 akhirnya NIST mempublikasikan AES sebagai standar pemrosesan dokumen pada dokumen FIPS-PUB 197, (NIST, 2001).

Algoritma ini termasuk jenis simetrik karena menggunakan kunci enkripsi dan kunci dekripsi yang sama. AES menggunakan sandi blok kunci simetrik dengan ukuran kunci yang bervariasi, antara lain AES 128, 192, 256 bit dengan panjang blok 128 bit. Penyandian AES menggunakan proses yang berulang disebut dengan *round*. Setiap blok dienkripsi dalam sejumlah putaran tertentu berdasarkan panjang kunci. Pada panjang kunci AES 128 bit membutuhkan 10 putaran, untuk kunci AES 192 bit membutuhkan 12 putaran. Sedangkan kunci AES 256 bit membutuhkan 14 putaran [2]. Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi *byte*, yaitu *SubBytes*, *ShiftRows*, *MixColoumns*, dan *AddRoundKey*. Kemudian proses dekripsinya menggunakan transformasi invers pada semua transformasi yang digunakan pada algoritma AES. Setiap transformasi dasar AES memiliki transformasi invers, yaitu: *InvSubBytes*, *InvSiftRows*, dan *InvMixColoumns*, sedangkan *AddRoundKey* bersifat *self-invers*.

Teori pengkodean merupakan ilmu tentang kode pendeteksi atau pengontrol kesalahan. Dengan kata lain digunakan sebagai pendeteksi dan pengoreksi kesalahan yang muncul saat data dikirim atau disimpan. Salah satu contoh teknik pengkodean adalah *Turbo Code*. *Turbo Code* pertama kali diperkenalkan oleh Berrou, Glavieux, dan Thitimajshima pada tahun 1993, dalam skema yang dapat mencapai probabilitas kesalahan bit sebesar 10^{-5} menggunakan laju $\frac{1}{2}$ pada kanal AWGN. Teknik pengkodean *Turbo Code* telah terbukti memberikan unjuk kerja mendekati teori Limit Shannon. Pada proses *encoding*-nya berupa rangkaian paralel dua atau lebih kode *Recursive Systematic Convolutional* (RSC) yang dipisahkan oleh *interleaver* [3]. Sedangkan pada proses *decoding*-nya yaitu meneruskan *soft decision* dari keluaran sebuah *decoder* ke masukan *decoder* berikutnya, dan mengulangi proses ini beberapa kali untuk menghasilkan keputusan yang lebih handal [4].

Metode kombinasi AES dan *Turbo Code* pernah diteliti oleh Hakan CAM, Volkan OZDURAN, dan Osman N UCAN dengan melakukan kombinasi antara enkripsi AES dan teknik pengkodean *Turbo Code* pada satu langkah diharapkan dapat menghasilkan keputusan yang efisien dan efektif. Dengan mengenkripsi dan mendekripsi data dengan menggunakan AES, sedangkan *Turbo code* digunakan untuk proses *encoding* dan *decoding*.

Pada penelitian ini, penulis menggunakan metode ini pada sisi enkripsi dengan menganalisis perbandingan kombinasi metode AES dan *Turbo Code* terhadap 3 kunci AES dengan variasi ukuran *frame* dengan parameter penguji yaitu BER (*Bit Error Rate*), dan *Avalanche Effect*.

1.2. Rumusan Masalah

1.2.1. Permasalahan

Adapun permasalahan yang ditemukan berdasarkan uraian diatas, yaitu apakah variasi ukuran *frame* dengan variasi kunci AES mempengaruhi efektifitas kombinasi metode AES – *Turbo Code*?

1.2.2. Metode Usulan

Adapun solusi yang diusulkan untuk menyelesaikan permasalahan yang disebutkan pada bagian 1.2.1 yaitu menerapkan kombinasi antara teknik kriptografi AES dan *Turbo Code* yang berfungsi sebagai pengoreksi kesalahan sehingga menghasilkan keputusan yang efektif.

1.2.3. Pertanyaan Penelitian

Berdasarkan latar belakang masalah yang telah dipaparkan diatas, maka penulis merumuskan permasalahan pada penelitian ini yaitu, bagaimana pengaruh efektifitas kombinasi metode AES dan *Turbo Code* pada 3 kunci AES terhadap variasi ukuran *frame* menggunakan data teks.

Tabel 1. 1. Perumusan Masalah

Masalah	Solusi	Pertanyaan penelitian	Tujuan Penelitian
Apakah variasi ukuran <i>frame</i> dengan variasi kunci AES mempengaruhi efektifitas kombinasi metode AES – Turbo Code?	Menerapkan kombinasi metode AES dan Turbo Code.	Bagaimana pengaruh efektifitas kombinasi metode AES dan Turbo Code pada 3 kunci AES terhadap variasi ukuran <i>frame</i> menggunakan data teks?	Untuk mengetahui pengaruh efektifitas dari metode AES dan Turbo Code pada 3 kunci AES terhadap variasi ukuran <i>frame</i> menggunakan data teks.

1.3. Tujuan dan Manfaat

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

1.3.1. Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah mengetahui pengaruh efektifitas kombinasi metode AES-Turbo pada 3 kunci AES terhadap variasi ukuran *frame*.

1.3.2. Manfaat Penelitian

Adapun manfaat yang diperoleh, sebagai berikut:

1. Bagi peneliti
 - a. Mampu menerapkan metode kriptografi AES dan teknik pengkodean Turbo Code.
 - b. Mengetahui efisiensi dan efektifitas kombinasi metode AES-Turbo pada 3 kunci AES terhadap variasi ukuran frame.
2. Bagi dunia pendidikan

Diharapkan dapat menjadi referensi pengetahuan dalam menerapkan kombinasi metode AES-Turbo.

1.4. Batasan Masalah

Batasan masalah dalam penelitian ini adalah :

1. Data yang diproses adalah data teks menggunakan ukuran data 300, dan 3190 karakter.
2. Panjang kunci yang digunakan yaitu 128 bit, 192 bit dan 256 bit.
3. Ukuran frame yang digunakan yaitu 128, 256, dan 384.
4. Parameter yang digunakan meliputi BER (*Bit Error Rate*), dan *Avalanche Effect*.
5. *Interleaver* yang digunakan pada *encoder* adalah *interleaver random*, *code rate* $r = \frac{1}{2}$ (*puncture*).
6. Jumlah iterasi *decoder* = 1, dan menggunakan *decoder* Log-Map.
7. Kanal berderau (*noise*) yang digunakan yaitu kanal AWGN dengan kondisi SNR 5 dB – 15dB sebagai parameter pembangkit *noise*.

1.5. Sistematika Penulisan

Dalam penelitian ini, sistematika penulisan yang digunakan terbagi menjadi lima bab dengan susunan sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini menjelaskan dasar-dasar dari penulisan laporan tugas akhir, yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan, metode penelitian serta sistematika penulisan laporan tugas akhir.

BAB 2 KAJIAN PUSTAKA

Bab ini membahas teori-teori yang berhubungan dengan topik penelitian, meliputi teknik kriptografi AES dan teknik pengkodean *Turbo Code*

BAB 3 METODE USULAN

Bab ini membahas tentang analisis proses enkripsi dan dekripsi algoritma AES dan teknik pengkodean *Turbo Code* yang terdiri dari *Flowchart* dan perancangan sistem, ujicoba dan analisis.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini membahas tentang hasil implementasi dan pengujian sistem serta pembahasan dari hasil yang diperoleh sesuai dengan analisis dan perancangan sistem yang dilakukan sebelumnya.

BAB 5 PENUTUP

Bab ini membahas tentang kesimpulan yang diperoleh dari hasil penelitian serta saran-saran yang ditujukan bagi para pembaca dan pengembang sistem untuk penelitian selanjutnya.