BAB 1
PENDAHULUAN

1.1 Latar Belakang

Penggunaan teknologi *wireless* sudah menjadi hal yang lumrah dalam kehidupan sehari – hari masyarakat dewasa ini. Mulai dari telepon genggam, hingga *Wireless Fidelity* (Wi-Fi) merupakan bagian dari teknologi ini. Semakin luasnya penggunaan teknologi ini, semakin banyak pula orang yang tertarik untuk memanfaatkan teknologi ini, baik dari sisi positif ataupun negatif.

Teknik enkripsi adalah bagian yang vital dalam sistem pengamanan kanal wireless. Pertukaran informasi pada jaringan wireless menggunakan ruang terbuka untuk media transmisi, sehingga hubungan wireless rentan terhadap tindakan yang berpotensi merugikan pengguna, misalnya interupsi dan pengubahan sebuah pesan dalam proses pengiriman pesan tersebut.

Algoritma *Data Encryption Standard* atau DES adalah salah satu teknik enkripsi yang biasa digunakan dalam pengamanan sebuah pesan dalam menghadapi serangan. Pengamanan pesan pada DES memenuhi *Avalanche Criterion* yakni pesan dienkripsi sedemikian rupa, agar 2 buah plainteks yang mirip, tidak akan menghasilkan cipherteks yang mirip juga. Hal ini baik bila pesan dikirim melalui jaringan kabel yang minim *noise*, namun pada komunikasi *wireless*, noise adalah bagian dari komunikasi itu sendiri. Sehingga, bila DES diimplementasikan pada komunikasi wireless, *Bit Error Rate* (BER) dari sistem tersebut akan besar dan merusak pesan yang dikirimkan.

Untuk mengatasi hal tersebut, algoritma DES dimodifikasi sehingga dapat mengurangi nilai BER dalam komunikasi *wireless*. Algoritma ini dikenal sebagai *Modified Data Encryption Standard Algorithm* atau bisa disebut Algoritma M-DES.

Dalam tugas akhir kali ini akan dibuat perbandingan antara algoritma DES murni dan algoritma M-DES untuk membuktikan bahwa algoritma M-DES memang dapat mengurangi nilai BER dan meningkatkan keamanan pesan.

1.2 Perumusan Masalah

Berdasarkan deskripsi latar belakang dan penelitian terkait, dapat dirumuskan beberapa masalah di tugas akhir ini yaitu :

1. Banyak tindakan pencurian dan atau peretasan pesan untuk mengetahui informasi informasi sensitif.
2. Metode yang dapat dilakukan adalah pengamanan pesan menggunakan algoritma kriptografi DES, namun terdapat kekurangan kekurangan jika hanya menggunakan algoritma standar.
3. Untuk meningkatkan keamanan pesan, algoritma kriptografi DES akan dimodifikasi dengan menambahkan proses untuk setidaknya mengurangi kelemahan algoritma DES standar.

1.3 Batasan Masalah

Berdasarkan latar belakang dan rumusan masalah, maka dibuatlah batasan batasan masalah di tugas akhir ini yaitu :

1. Sistem dirancang hanya mengenai proses enkripsi, penyisipan pesan pada citra, ekstraksi pesan, dan dekripsi tanpa melalui media transmisi.
2. Menggunakan perangkat matlab R2013a
3. Input percobaan berupa *plaintext* dengan panjang 32 dan 64 karakter.
4. Parameter yang diteliti adalah BER, *avalanche effect*, dan waktu komputasinya.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah :

1. Meningkatkan keamanan pesan dan menghambat proses peretasan pesan
2. Enkripsi data berupa teks menggunakan algoritma kriptografi DES yang telah dimodifikasi untuk meningkatkan keamanan data teks.
3. Mengimplementasikan metode kriptografi menggunakan algoritma DES yang telah di modifikasi dalam mengamankan data berupa teks dengan bahasa pemrograman *Fortran* pada aplikasi matlab R2013a.
4. Mengetahui performa kriptografi menggunakan algoritma DES yang telah dimodifikasi.

1.5 Metodologi Penelitian

Metodologi dalam proses penyelesaian penelitian ini terdiri dari :

1. Studi literatur, yaitu dengan mempelajari materi yang berhubungan dengan tugas akhir ini, baik dari *textbook,* jurnal, maupun diskusi dengan pihak - pihak berkompeten.
2. Eksperimen, yaitu dengan melakukan uji coba pembuatan program dari tahap sebelumnya.
3. Pemodelan dan implementasi, yaitu pembuatan aplikasi yang sesuai dengan topik dan menerapkan konsep yang telah ditentukan.
4. Pengujian dan analisa, yaitu pengujian aplikasi yang telah dibuat dengan dasar yang telah ditentukan pada batasan masalah sehingga menghasilkan output, kemudian melakukan analisa terhadap output, untuk dibandingkan dengan hipotesa.
5. Penulisan dan penyusunan laporan tugas akhir.

1.6 Sistematika Penulisan

1 BAB I PENDAHULUAN

Bab ini berisi uraian mengenai latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian, dan sistematika penulisan.

2 BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang teori yang berhubungan dengan Kriptografi, dan metode - metode yang akan digunakan dalam penelitian ini.

3 BAB III DESAIN MODEL SISTEM DAN SKENARIO EVALUASI

Bab ini dibahas tentang tahap - tahap perancangan sistem pengamanan pesan menggunakan algoritma DES yang telah dimodifikasi.

4 BAB IV PENGUJIAN DAN ANALISIS

Bab ini dijelaskan mengenai hasil dari pengujian sistem yang telah dibuat dengan menganalisis parameter yang digunakan dan mempengaruhi hasil pengujian sistem.

5 BAB V KESIMPULAN, SARAN, DAN PENUTUP

Bab ini membahas tentang kesimpulan yang dapat ditarik dari pembuatan tugas akhir ini dan kemungkinan pengembangan topik yang bersangkutan.