

BAB I

PENDAHULUAN

1. 1. Latar Belakang

Pada saat ini kejahatan dalam pengiriman pesan baik itu berupa teks, data, suara maupun gambar sangat sering terjadi. Setiap orang sudah tidak bisa merasakan kenyamanan dalam berkomunikasi, karena pesan yang mereka kirimkan setiap waktu bisa saja diketahui oleh pihak-pihak yang tidak berkepentingan. Oleh karena itu diperlukan suatu metode pengamanan yang dapat dipercaya.

Pengamanan data dapat dilakukan dengan berbagai cara, antara lain kriptografi dan steganografi. Dengan menggunakan metode kriptografi saja hasil enkripsi data akan dicurigai oleh orang awam yang membacanya, karena hasil kriptografi tersebut terlihat aneh dan berantakan. Sehingga perlu adanya suatu metode agar data hasil enkripsi tersebut terlihat seperti data normal. Dengan menggunakan metode steganografi memungkinkan seseorang untuk mengirimkan sebuah pesan dengan menyisipkan pesan ke data lain (teks, suara, gambar), sehingga dapat menghindari kecurigaan pihak lain tentang data yang dikirimkan. Tetapi setelah pihak ketiga dapat mengekstrak pesan dari media steganografi pesan akan langsung didapatkan. Untuk memperbaiki kekurangan tersebut maka dapat digunakan gabungan kedua metode kriptografi dan steganografi.

Pada tugas akhir ini dirancang sebuah aplikasi yang dapat memenuhi kebutuhan pengamanan data seperti yang disebutkan diatas, yaitu pengamanan data berupa teks yang dimanipulasi menggunakan metode kriptografi AES dan steganografi *Spread Spectrum* ke dalam sebuah citra digital berbasis bahasa pemrograman Java. Aplikasi ini memiliki fungsi sebagai enkoder untuk sisi pengiriman data dan dekoder untuk sisi penerima data. Sehingga diharapkan aplikasi ini dapat menjadi salah satu pilihan untuk mengamankan data teks di dalam sebuah lingkungan yang rentan terhadap serangan informasi berupa *eavesdropping*.

1. 2. Tujuan Masalah

Adapun tujuan dari penelitian tugas akhir ini adalah:

1. Mendesain dan membangun aplikasi pengamanan data teks dengan algoritma AES dan *Spread Spectrum* dengan bahasa Java.
2. Menguji aspek *recovery, robustness, security*.

1. 3. Rumusan Masalah

Dalam tugas akhir ini dirumuskan masalah sebagai berikut:

1. Bagaimana mendesain dan membangun aplikasi pengamanan data teks dengan algoritma AES dan *Spread Spectrum* dengan bahasa Java.
2. Bagaimana menguji aspek *recovery, robustness, security*.

1. 4. Batasan Masalah

Untuk mendapatkan hasil yang spesifik sesuai dengan yang diinginkan, dalam penelitian kali ini ditentukan batasan masalah sebagai berikut:

1. Data yang akan dienkripsi berupa data teks.
2. Algoritma yang digunakan untuk melakukan kriptografi adalah AES.
3. Metode yang digunakan untuk melakukan steganografi adalah *Spread Spectrum*.
4. Data cipherteks dari kriptografi disisipkan pada data citra digital.
5. Aplikasi ini hanya berfungsi untuk menerjemahkan plainteks ke cipherteks kemudian disisipkan ke citra dan sebaliknya, sesuai dengan algoritma yang digunakan.

1. 5. Metode Penelitian

Penelitian ini akan dilakukan dalam beberapa tahap, yaitu:

1. Studi literatur
Pengumpulan dan pemahaman literatur berupa jurnal ilmiah, buku referensi, dan jurnal dari internet yang mendukung penyusunan tugas akhir ini.
2. Perancangan aplikasi
Melakukan perancangan sistem yang akan dibuat, meliputi perancangan antarmuka, maupun aplikasi sebagai enkoder dan aplikasi sebagai dekoder

dengan metode kriptografi AES dan steganografi *Spread Spectrum* dengan bahasa pemrograman Java.

3. Tahap realisasi

Melakukan realisasi pada sistem yang dirancang meliputi pembuatan pembangunan antarmuka dan aplikasi sebagai dekoder dengan metode kriptografi AES dan steganografi *Spread Spectrum* dengan bahasa pemrograman Java..

4. Tahap pengujian

Melakukan pengujian dan realisasi sistem

5. Tahap analisis dan penarikan kesimpulan

Melakukan analisis dari data yang telah didapatkan dari hasil pengujian.

1. 6. Sitematika Penulisan

Sistematika penulisan pada proposal tugas akhir inidibagi menjadi beberapa bab yang meliputi:

BAB I PENDAHULUAN

Pendahuluan berisi latar belakang, tujuan penelitian, rumusan masalah, batasan masalah, metode penelitian dan sistematika penulisan.

BAB II DASAR TEORI

Pada bab ini, membahas teori mengenai keamanan data, kriptografi, AES, steganografi, dan *Spread Spectrum*.

BAB III PERANCANGAN SISTEM

Pada bab ini, membahas tentang perancangan antarmuka, proses perancangan sistem, dan proses aliran data.

BAB IV ANALISA DAN PENGUJIAN

Pada bab ini, akan dibahas mengenai mengenai implementasi dan analisis hasil pengujian aplikasi dari sisi user.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang didapat selama pengerjaan Tugas Akhir serta saran bagi pengembangan di masa mendatang.