BAB 1 PENDAHULUAN

1.1. Latar Belakang

Seiring dengan perkembangan teknologi informasi, semakin berkembang juga kejahatan seperti pencurian informasi oleh pihak yang tidak diizinkan secara tidak sah, pada saat ini kejahatan siber menjadi yang paling dikenal oleh kalangan umum. Dari masalah yang terjadi seperti kebocoran informasi yaitu kegagalan dalam melindungi data pribadi, seperti masalah pada sektor perbankan. Data pribadi digunakan untuk melakukan tindakan kejahatan oleh pihak yang tidak diizinkan dalam penipuan yang marak terjadi [1]. Otoritas Jasa Keuangan (OJK) melaporkan kenaikan angka kejahatan yang terjadi di Indonesia pada tahun 2020 hingga 2023 yang dikonfirmasi lebih dari 20 tindakan kejahatan yang menyebabkan kebocoran informasi mengenai nasabah dari banyak bank yang menunjukkan ketidaksiapan dalam menghadapi perkembangan teknologi yang terjadi pada saat ini dari sektor perbankan, yang menyebabkan kerugian dari sisi finansial untuk nasabah serta lembaga perbankan degan total triliunan rupiah [2]. Keamanan data saat ini menjadi peran yang vital pada kemajuan teknologi yang terjadi agar tidak di salahgunakan oleh pihak yang tidak sah dan juga untuk mengurangi risiko kebocoran informasi yang dianggap penting, salah satu teknik untuk mengamankan informasi penting yaitu kriptografi dan steganografi yang bisa digunakan sebagai keamanan ganda untuk menjaga informasi secara rahasia dan penyembunyian informasi digital [3].

Kriptografi digunakan untuk cara pengamanan informasi dengan cara mengubah informasi penting menjadi tidak dapat terbaca berupa cipertext. Salah satu algoritma kriptografi yaitu Advanced Encryption Standard(AES). Kriptografi dibedakan mejadi dua tipe yaitu simetris dan asimetris, untuk tipe simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, sedangkan tipe asimetris menggunakan kunci yang berbeda [4],[5]. Pada kriptografi bentuk chipertext yang tidak terbaca bisa mudah dikenali disadari, sehingga dilakukan kombinasi antara kriptografi dan steganografi dengan cara menyembunyikan informasi rahasia yang dihasilkan ke dalam media penampung dengan memasukkan informasi ke dalamnya [6].

Berbeda dengan kriptografi yang mengubah isi pesan, Steganografi berguna sebagai cara mengaburkan informasi dengan maksud tidak menimbulkan kecurigaan. Steganografi digunakan dengan dua sarana, yaitu informasi dan sarana penyimpanan. Sarana penyimpanan yang umum digunakan pada saat ini seperti Audio, Gambar, atau Video, sedangkan informasi yang dimasukkan seperti file PDF, Word maupun bentuk yang lain [7], [8]. Salah satu metode steganografi adalah *spread spectrum*, secara penggunaannya penyisipan dan pengambilan informasi dari *spread spectrum* terdiri dari tiga langkah, untuk penyisipan informasi di awali dengan cara penyebaran, modulasi dan penyisipan pesan, sedangkan untuk langkah pengambilan informasinya di awali dengan cara pengambilan pesan yang ada, demodulasi, dan penyusutan pesan [9].

Dari uraian yang telah di sampaikan, penulis berusaha menjalankan gabungan kriptografi dan steganografi untuk pengamanan informasi pada sarana digital, menggunakan algoritma kriptografi simetris yaitu algoritma Advanced Encryption Standart (AES) untuk enkripsi dan dekripsi informasi dan metode steganografi *spread spectrum* sebagai metode penyisipan, yang memiliki tujuan akan keberhasilan dari gabungan algoritma AES dan *spread spectrum* sebagai sarana pengamanan informasi yang diharapkan dapat memberikan kontribusi dalam memperkecil tindakan kejahatan yang menyebabkan kebocoran informasi.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah di uraikan, rumusan masalah pada penelitian ini yaitu menerapkan algoritma Advanced Encryption Standart (AES) untuk mengetahui keberhasilan dari gabungan algoritma tersebut dengan metode Steganografi *Spread Spectrum* sebagai langkah untuk pengamanan data digital.

1.3. Tujuan dan Manfaat

1. Menerapkan algoritma AES untuk enkripsi dan deskripsi pesan
2. Memberikan pengetahuan penerapan Algoritma AES untuk enkripsi dan deskripsi pdf

1.4. Batasan Masalah

Berdasarkan rumusan masalah dan tujuan penelitian yang telah di uraikan, untuk mewujudkan penelitian yang sesuai dengan masalah yang ada diperoleh batasan-batasan masalah penelitian sebagai berikut:

1. Pesan yang digunakan merupakan file format (*.pdf).
2. Algoritma yang diterapkan pada proses enkripsi dan deskripsi menggunakan Algoritma AES
3. Metode steganografi yang digunakan pada penelitian ini yaitu *Spread Spectrum* dengan media file citra berformat (*.PNG).

1.5. Metode Penelitian

Penelitian ini dimulai dengan mengindifikasi masalah yang berfokus pada penggabungan Algoritma AES dengan Steganografi *Spread Spectrum*, kemudian mencari studi literatur dengan mempelajari penelitian sebelumnya tentang Kriptografi, AES, dan steganografi. Selanjutnya perancangan sistem untuk implementasi penelitian serta pengujian untuk memastikan sistem berjalan dengan baik. Lalu pada tahap terakhir melakukan analisis dari hasil yang telah dijalankan pada sistem dan penulisan laporan.