BAB I
PENDAHULUAN

1.1 Latar Belakang

Era digital mentransformasi cara manusia berkomunikasi, berbisnis, dan menyimpan informasi. Pertukaran data digital kian masif, membawa kemudahan sekaligus memicu kecemasan terkait keamanan data. Kebocoran data dan penyalahgunaan informasi menjadi ancaman nyata yang dapat mengakibatkan kerugian finansial, reputasi, bahkan pelanggaran privasi. Kriptografi, metode keamanan data tradisional, telah terbukti efektif dalam melindungi data. Namun, kriptografi dapat menarik perhatian pihak yang tidak berwenang, meningkatkan risiko investigasi dan penyadapan. Steganografi, sebuah teknik menyembunyikan data rahasia di dalam media lain (*carrier*), menawarkan solusi keamanan yang lebih canggih. Data rahasia tersembunyi tidak terdeteksi, sehingga meningkatkan keamanan dan privasi informasi[1].

Kebutuhan akan keamanan informasi yang semakin meningkat dalam era digital. Informasi perlu disembunyikan secara efektif atau dilindungi dari penyalahgunaan dengan menambahkan watermark atau metadata[2].

Internet telah menjadi saluran komunikasi yang paling disukai saat ini, di mana hampir semua dokumen seperti teks, gambar, audio, atau video, ditransmisikan melalui internet. Hal ini menunjukkan bahwa keamanan dalam mentransfer data melalui internet menjadi semakin penting, terutama dalam mengamankan informasi rahasia dari pihak yang tidak berwenang. Steganografi audio berbasis LSB (*Least Significant Bit*) merupakan salah satu teknik yang digunakan untuk menyembunyikan data rahasia dalam file audio digital. Teknik ini memanfaatkan bit paling tidak signifikan dalam sampel audio untuk menyisipkan informasi rahasia tanpa mengubah secara signifikan kualitas audio yang terdengar. Dengan menggunakan teknik ini, informasi sensitif dapat disembunyikan secara efektif dalam file audio tanpa diketahui oleh pihak yang tidak berhak[3].

Penyisipan LSB memanfaatkan bit paling tidak signifikan dari data host untuk menyembunyikan informasi tambahan, sehingga perubahan yang dihasilkan pada

data host tidak terlalu mencolok secara visual. Teknik ini memungkinkan pengguna untuk menyembunyikan pesan rahasia dalam data host tanpa mengganggu kualitas visual atau audio dari media tersebut. Dalam konteks keamanan informasi, steganografi dapat digunakan dalam berbagai aplikasi seperti komunikasi rahasia, pertukaran data sensitif, dan pengamanan informasi penting. Dengan menggunakan teknik steganografi, pengguna dapat meningkatkan keamanan data mereka dengan cara yang tidak terlihat oleh pihak yang tidak berwenang[4].

Kriptografi adalah sebuah teknik yang digunakan untuk mengamankan pesan-pesan yang dikirim melalui platform berbasis ponsel pintar. Kriptografi melibatkan proses enkripsi dan dekripsi pesan, di mana pesan asli diubah menjadi bentuk yang tidak dapat dibaca (*ciphertext*) sebelum dikirim, dan kemudian diubah kembali menjadi pesan asli saat diterima. Algoritma kriptografi dibagi menjadi 2 yaitu Simetris dan Asimetris. Algoritma simetris merupakan suatu algoritma yang menggunakan single key untuk melakukan enkripsi maupun dekripsi pesan atau sering disebut single key. Algoritma ini banyak digunakan untuk enkripsi dan dekripsi pesan karena kelebihannya yaitu simple dan cepat. Disisi lain kekurangan yang dimiliki algoritma ini yaitu jika key yang digunakan untuk enkripsi dan dekripsi pesan diketahui oleh pihak selain pengirim, penerima maka segala informasi didalamnya akan diketahui juga. Contoh dari algoritma ini yaitu AES, RC4, Blowfish, *Rijndael*. Algoritma asimetris merupakan suatu algoritma kriptografi yang sering disebut *public key*. Algoritma ini memiliki 2 kunci yaitu *public key* dan *private key* sehingga berbeda untuk kunci untuk enkripsi dan dekripsi pesan. Kunci publik dapat dilihat untuk umum karena untuk pengirimannya tidak perlu pada saluran dengan keamanan tinggi sedangkan kunci privat dimiliki oleh masing-masing pengirim dan penerima. Kelebihan daripada algoritma asimetris ini yaitu jumlah kunci dapat ditekan untuk masing-masing penerima karena tidak perlu membuat kunci sebanyak algoritma simetris yang berbeda untuk masing-masing penerima. Contoh dari Algoritma ini yaitu ECC (Elliptic Curve Cryptography), Paillier. Penggabungan steganografi dan kriptografi secara bersamaan dapat meningkatkan pengamanan data. Metode penggabungan steganografi dan

kriptografi banyak dikembangkan. Pada umumnya teknik yang digunakan yaitu dengan mengenkripsi pesan terlebih dahulu (kriptografi), kemudian menyisipkannya ke media cover (steganografi)[5].

Manajemen key pada algoritma *asymmetric encryption* lebih sederhana, terutama untuk pengiriman dara melalui internet. Namun hanya dapat digunakan untuk data berukuran kecil. Salah satu algoritma *asymmetric encryption* adalah Elliptic Curve Cryptography (ECC). ECC menyediakan keamanan dengan tinggi dengan ukuran kunci yang lebih kecil dibandingkan dengan metode kriptografi yang lain[6]. Sedangkan Pada algoritma paillier *cryptosystem* proses enkripsinya dilakukan per-karakter. Selain itu, salah satu kelebihan dari Algoritma Paillier Cryptosystem adalah adanya sifat homormofisme dan self-blinding. Beberapa sifat inilah yang membuat algoritma paillier cryptosystem dapat dipergunakan untuk berbagai keperluan, salah satunya untuk pengamanan pesan teks[7].

Media audio yang digunakan steganografi audio pada penelitian ini berformat aiff dan wav. Karena wav dan aiff bisa dibilang merupakan format file audio tidak terkompresi yang paling populer, keduanya berbasis PCM (Pulse Code Modulation), yang dikenal luas sebagai mekanisme penyimpanan audio paling mudah dalam ranah digital. Sehingga dapat menyembunyikan file pesan *chipertext* dengan ukuran cukup besar dan dapat diekstrak kembali sesuai dengan bit yang disembunyikan[8].

Nilai hash adalah suatu kode alfanumerik yang dihasilkan dari suatu data tertentu. Hash digunakan untuk menghasilkan representasi digital kecil dari data yang lebih besar. Proses hash ini mengubah data menjadi kombinasi angka, huruf, atau karakter lain yang terenkripsi. MD5 merupakan singkatan dari Message Digest Algorithm 5[9].

Dari uraian diatas, penulis akan menerapkan algoritma kriptografi asimetris yaitu Algoritma ECC dan Paillier untuk enkripsi dan dekripsi pesan sehingga dapat mengetahui algoritma mana yang lebih efektif digunakan dalam upaya pengamanan pesan dalam sisipan file pada format file audio AIFF dan WAV dengan

menggunakan metode LSB (*Least Significant Bit*), kemudian digabungkan dengan MD5 hash untuk memastikan keaslian data.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat diiidentifikasikan menjadi rumusan masalah pada penelitian ini yaitu :

1. Bagaimana algoritma ECC dan Paillier dapat diterapkan untuk enkripsi dan dekripsi keamanan pesan?
2. Bagaimana mengimplementasikan metode steganografi LSB untuk menyembunyikan pesan teks di dalam audio?
3. Bagaimana cara menggunakan algoritma MD5 Hash untuk menguji integritas pesan?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka diketahui tujuan penelitian antara lain :

1. Membandingkan algoritma ECC dan Paillier, untuk mengetahui algoritma mana yang terbaik dalam implementasi enkripsi dan dekripsi pesan.
2. Untuk menyisipkan pesan, metode steganografi (Least Significant Bit) LSB diterapkan agar tidak disalahgunakan oleh orang lain.
3. Mengimplementasikan algoritma MD5 hash.

1.4 Batasan Masalah

Berdasarkan rumusan masalah dan tujuan penelitian, maka untuk melakukan penelitian berdasarkan permasalahan yang ada, maka ditetapkan batasan masalah dalam penelitian ini sebagai berikut :

1. Metode steganografi yang digunakan adalah Least Significant Bit (LSB).
2. Algoritma yang diterapkan pada enkripsi dan dekripsi pesan ini menggunakan Algoritma Nirsimetris/Asimetris yaitu Algoritma ECC (Elliptic Curve Cryptography) dan Algoritma Paillier.

3. Format audio yang digunakan sebagai media menyembunyikan teks bertipe .AIFF dan .WAV mengevaluasi keamanan dan ketahanan metode LSB terhadap serangan steganalisis.
4. Pesan yang digunakan untuk penyisipan pada penelitian ini berupa file (*.pdf).
5. Algoritma yang digunakan untuk menguji integritas file yaitu MD5 hash.
6. Metode yang digunakan untuk menganalisis antar kedua algoritma adalah nilai MSE, dan PNSR.

1.5 Manfaat Penelitian

Berdasarkan rumusan masalah di atas, manfaat penelitian adalah sebagai berikut :

1. Mengembangkan pemahaman tentang penyisipan pesan dengan menerapkan proses steganografi menggunakan metode LSB (Least Significant Bit) yang menggunakan dua algoritma kriptografi yaitu algoritma ECC dan Paillier.
2. Mampu menggunakan metode Least Significant Bit (LSB) untuk menyembunyikan pesan, agar pesan tetap rahasia.
3. Meningkatkan sistem pengamanan pesan, supaya pesan yang diterima dapat dipercaya karena aman, rahasia, dan akurat.

1.6 Rencana Kegiatan

Rencana kegiatan dalam penelitian ini meliputi langkah-langkah berikut :

1. Kajian Pustaka

Tahap awal dilakukan dengan mempelajari teori-teori yang relevan, mencakup konsep dasar algoritma ECC dan Paillier, steganografi, kriptografi, metode penyisipan LSB, serta metode evaluasi keamanan seperti MSE dan PSNR. Studi ini diperoleh dari buku referensi, jurnal ilmiah, dan penelitian sebelumnya.

2. Pengumpulan Data

Pada tahap ini dilakukan identifikasi terhadap kebutuhan input (file .pdf, audio .wav dan .aiff), proses (enkripsi, penyisipan, dekripsi), dan output (file stego, ciphertext, hasil hash MD5), yang akan menjadi dasar dalam perancangan sistem.

3. Perancangan Sistem

a. Proses Enkripsi

Dilakukan dua kali enkripsi yaitu menggunakan algoritma ECC dan Paillier untuk membandingkan efektivitasnya.

b. Penyisipan Pesan

Ciphertext yang telah terenkripsi disisipkan ke dalam file audio menggunakan metode Least Significant Bit (LSB).

c. Pembuatan Hash MD5

Untuk memastikan keaslian pesan, dilakukan proses hashing terhadap file stego.

d. Proses Dekripsi

Setelah file stego diekstrak, algoritma yang sama digunakan untuk mendekripsi kembali ciphertext untuk mendapatkan pesan asli.

4. Pengujian dan Analisis Data

Pengujian dilakukan untuk membandingkan hasil penggunaan kedua algoritma dari sisi besar data file, kecepatan proses, serta kualitas audio hasil steganografi menggunakan perhitungan MSE dan PSNR.

5. Kesimpulan

Berdasarkan hasil analisis, kesimpulan dapat diambil dari efektivitas penggunaan algoritma ECC dan Paillier dalam konteks steganografi audio. Rekomendasi atau saran juga diberikan mengenai hasil analisis sebelumnya.