BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah mempermudah proses pertukaran pesan dan informasi. Dalam proses ini, menjaga keamanan data menjadi sangat penting untuk mencegah akses oleh pihak yang tidak berwenang. Di era digital ini masyarakat dapat dengan mudah mengakses, mengumpulkan, dan bertukar informasi secara cepat dan bebas melalui internet. Kebebasan ini juga membuka peluang bagi kejahatan siber seperti akses tidak sah terhadap data dan penyalahgunaan informasi untuk keuntungan pribadi yang merugikan pengguna internet. Oleh karena itu keamanan data menjadi krusial untuk menjaga kerahasiaan dan integritas informasi dari berbagai ancaman siber (Siambaton, 2023).

Kriptografi adalah ilmu yang bertujuan menjaga kerahasiaan pesan dengan mengubahnya menjadi bentuk yang tidak dapat dipahami (Rafli, 2024). Kriptografi pertama kali digunakan oleh bangsa Mesir sekitar tahun 3000 SM. Kata kriptografi berasal dari bahasa Yunani, yaitu *kryptos* yang berarti "tersembunyi" dan *graphia* yang berarti "tulisan". Perbedaan utama antara berbagai teknik kriptografi terletak pada metode penyandiannya. Semakin kompleks metode yang digunakan, semakin sulit bagi pihak tidak berwenang untuk memecahkan kode pengamanan pesan tersebut (Hani, 2020).

Kriptografi dapat dibagi menjadi dua kategori utama yaitu kriptografi simetris dan kriptografi asimetris. Kriptografi simetris menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi. Sebaliknya, kriptografi asimetris menggunakan dua kunci yang berbeda, satu untuk enkripsi dan satu lagi untuk dekripsi (Cahyani, 2022).

Algoritma ElGamal termasuk dalam kategori algoritma asimetris karena menggunakan kunci yang berbeda dalam proses enkripsi dan dekripsi. Algoritma

ElGamal diciptakan oleh Taher ElGamal pada tahun 1984. Kekuatan algoritma ini terletak pada perhitungan logaritma diskrit pada modulo bilangan prima yang besar (Cahyani, 2022). Algoritma ini pertama kali diterapkan untuk tanda tangan digital, namun kemudian dimodifikasi untuk enkripsi dan dekripsi data (Fauzi, 2023).

Kriptografi dapat menyamarkan pesan sehingga maksud dari pesan tersebut tidak dapat dipahami, tetapi pesan tersebut masih dapat terlihat sehingga para peretas mengetahui adanya pesan rahasia. Agar pesan rahasia tidak diketahui keberadaannya, pesan rahasia tersebut dapat disembunyikan dengan menggunakan steganografi. Meskipun demikian, keduanya tidaklah cukup aman secara mandiri. Namun, dengan menggabungkan keduanya, kita dapat meningkatkan keamanan dan kerahasiaan. Steganografi menyembunyikan data dalam *file* non-rahasia, seperti gambar, video, teks, atau audio. Untuk menggabungkan kedua teknik ini, data harus dienkripsi terlebih dahulu sebelum digunakan dalam prosedur steganografi untuk menciptakan cipherteks yang baru (Sabaya, 2023).

Steganografi adalah ilmu yang mempelajari teknik untuk menyembunyikan pesan rahasia di dalam media seperti gambar, video, teks, atau audio tanpa menimbulkan kecurigaan (Nurhasanah, 2023). Penggunaan steganografi dalam gambar digital menjadi menarik karena kemampuan gambar untuk menyimpan banyak informasi tanpa mempengaruhi tampilan visualnya secara signifikan. Salah satu teknik yang umum digunakan dalam steganografi gambar adalah *Least Significant Bit* (LSB), di mana pesan disisipkan dalam gambar dengan mengubah *bit* terakhir setiap *byte*, tanpa terdeteksi mata manusia, meskipun sebagian *bit* diubah (Aziz, 2024).

Ada beberapa varian dalam metode LSB yaitu *sequential* dan acak. Pada metode *sequential*, *bit* pesan disembunyikan mulai dari piksel pertama sampai piksel terakhir. Pada metode acak, *bit* pesan tidak disembunyikan secara berurutan melainkan secara acak (Munir, 2024). Untuk menggunakan metode ini diperlukan *pseudorandom number generator* yang digunakan untuk membangkitkan bilangan acak.

Pada tahun 1982, M. Blum mengeksplorasi penerapan bilangan bulat Blum

dalam *bit pseudorandom*, dan bilangan bulat tersebut diberi nama sesuai dengan namanya. Kemudian, pada tahun-tahun berikutnya, algoritma *Blum Blum Shub* (BBS), yang menggunakan generator kuadrat, diciptakan oleh L. Blum, M. Blum, dan M. Shub (Joey, 2023).

Penelitian mengenai kriptografi ElGamal telah dilakukan oleh Firdaus (2017) yang hasilnya menunjukkan bahwa peningkatan algoritma RSA dan penggabungannya dengan algoritma ElGamal, dapat mempermudah proses penyandian pesan dan meningkatkan kesulitan penyadap dalam memecahkan pesan rahasia. Penelitian tersebut hanya menggunakan algoritma kriptografi RSA dan ElGamal, namun penelitian tersebut belum menggunakan metode steganografi sebagai teknik penyembunyian hasil enkripsi yang dihasilkan.

Pada tahun 2023, Saragih, Siregar, dan Dafitri melakukan penelitian dengan judul "Implementasi Penyisipan Pesan Teks Terenkripsi Menggunakan Kriptografi ElGamal pada Citra Digital Menggunakan Steganogarafi LSB." Dalam penelitian ini, metode LSB yang digunakan adalah sequential untuk menyisipkan pesan teks ke dalam citra digital. Penelitian yang dilakukan oleh Hidayat pada tahun 2013 menunjukkan bahwa kemampuan penyisipan pesan menggunakan metode steganografi LSB secara acak lebih unggul daripada metode sequential dalam hal keamanan dikarenakan penyisipan pesan secara acak lebih sulit dideteksi. Hal ini menjadi dasar pemikiran bahwa metode LSB *sequential* memiliki kelemahan dalam hal perlindungan data.

Penelitian oleh Naufal (2021) juga relevan, algoritma *Blum Blum Shub* (BBS) digunakan untuk menghasilkan bilangan acak yang menggantikan nilai pergeseran konstan pada algoritma Affine *Cipher*, meningkatkan keamanan kriptografi audio. Sementara itu, Ardhiansyah (2023) mengkaji implementasi kombinasi LSB dan BBS dengan Kriptografi Vigenere *Cipher* untuk penyisipan pesan rahasia dalam gambar. Metode kriptografi yang digunakan adalah algoritma Vigenere *Cipher* yang merupakan kriptografi simetris. metode ini memiliki kelemahan utama yaitu penggunaan kunci yang sama untuk enkripsi dan dekripsi. Penggunaan kunci yang sama meningkatkan

risiko keamanan karena jika kunci tersebut diketahui oleh pihak yang tidak berwenang, pesan dapat dengan mudah didekripsi. Sebaliknya, kriptografi asimetris menawarkan tingkat keamanan yang lebih tinggi melalui penggunaan pasangan kunci privat dan kunci publik. Dalam kriptografi asimetris, kunci publik dapat dibagikan secara bebas tanpa membahayakan keamanan pesan, karena hanya kunci privat yang sesuai yang dapat digunakan untuk mendekripsi pesan yang dienkripsi dengan kunci publik tersebut (Arif, 2023). Hal ini berarti bahwa meskipun kunci publik diketahui oleh pihak ketiga, mereka tidak dapat mendekripsi pesan tanpa akses ke kunci privat.

Penelitian ini berfokus pada pengembangan dari peningkatan keamanan dengan menggunakan algoritma kriptografi ElGamal yang digabungkan dengan steganografi *Least Significant Bit* dan *Blum Blum Shub* dalam mengamankan pesan dengan cara mengenkripsi pesan memakai metode kriptografi ElGamal lalu menyembunyikan hasil enkripsi ke dalam objek gambar dengan metode *Least Significant Bit* disisipkan secara acak menggunakan Algoritma *Blum Blum Shub*. Oleh karena itu, judul yang diambil dalam penelitian ini adalah "Implementasi Kriptografi ElGamal dan Steganografi Kombinasi *Least Significant Bit* dan *Blum Blum Shub* untuk Pengamanan Pesan Rahasia dalam Gambar".

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang yang telah dijabarkan maka dapat dirumuskan permasalahan untuk diselesaikan pada penelitian ini antara lain:

1. Bagaimana model kriptografi Elgamal dan steganografi kombinasi *Least Significant Bit* dan *Blum Blum Shub* untuk pengamanan pesan rahasia dalam gambar?
2. Bagaimana konstruksi program aplikasi kriptografi ElGamal dengan metode steganografi LSB dan *Blum Blum Shub* untuk pengamanan pesan rahasia dalam gambar?
3. Bagaimana perbandingan nilai *Peak Signal-to-Noise Ratio* antara *stego-*

image dan *cover-image* dalam mengetahui kualitas *stego-image*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, maka tujuan dari penelitian ini adalah:

1. Merancang algoritma kriptografi ElGamal pada Steganografi gambar dikombinasikan dengan metode *Least Significant Bit* dan *Blum Blum Shub*.
2. Mengonstruksi kriptografi Elgamal dan steganografi kombinasi *Least Significant Bit* dan *Blum Blum Shub* untuk pengamanan pesan rahasia dalam gambar.
3. Mengetahui kualitas *stego-image* berdasarkan hasil nilai *Peak Signal-to-Noise Ratio* antara *stego-image* dan *cover-image*.

1.4 Batasan Masalah

Batasan masalah yang digunakan pada penelitian ini adalah:

1. Cover media yang digunakan dalam penelitian ini adalah gambar berwarna *Red, Green,* dan *Blue (RGB)* dengan format *file* *.png
2. Pesan yang digunakan berupa data teks yang terdiri dari karakter-karakter yang termasuk dalam rentang ASCII 32 hingga 126.
3. *File* Pesan yang digunakan saat steganografi dalam penelitian ini berformat .txt
4. Pembangkitan kunci ElGamal dilakukan secara otomatis sehingga memerlukan batasan karakter maksimal yang ditentukan sebelum dilakukan enkripsi.

1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan pada penelitian ini antara lain:

1. Menerapkan dan mengembangkan ilmu pengetahuan tentang metode kriptografi elgamal dikombinasi dengan steganografi *Least Significant Bit* dan *Blum Blum Shub*.
2. Memudahkan pengamanan pesan menggunakan metode kriptografi elgamal dan kombinasi steganografi *Least Significant Bit* dan *Blum Blum Shub* dengan program aplikasi.