BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, perkembangan teknologi komunikasi dan informasi telah menjadi tren dalam kehidupan masyarakat. Tren menunjukkan bahwa evolusi teknologi tidak hanya disertai dengan kemajuan, tetapi juga dengan munculnya pola dan variasi kejahatan *cyber crime* yang baru (Danuri, 2019). Informasi digital juga semakin banyak digunakan dalam berbagai bidang kehidupan. Karena perkembangan teknologi informasi yang semakin pesat, keamanan informasi menjadi hal yang penting untuk diperhatikan. Hal ini karena informasi yang tidak aman dapat diakses oleh orang yang tidak berhak atau tidak bertanggung jawab, sehingga keakuratan dan kebenaran informasi tersebut dapat diragukan, bahkan menjadi informasi yang menyesatkan.

Perkembangan teknologi informasi telah menyebabkan meningkatnya jumlah informasi yang disimpan dalam media elektronik. Salah satu aspek penting dalam penyimpanan informasi adalah cara aksesnya, yang biasa disebut pengambilan informasi. Hak akses ditentukan oleh si pembuat informasi, artinya informasi tersebut hanya boleh didapatkan dengan sepengetahuan si pembuat informasi. Di sinilah perlunya peran sistem keamanan data dalam proses pengiriman informasi tersebut. Dibutuhkan suatu sistem untuk melindungi komunikasi, terutama untuk jenis komunikasi yang bersifat rahasia. Keamanan tersebut bertujuan untuk melindungi media komunikasi, teknologi komunikasi, dan kontennya (Nurul dkk., 2022).

Hingga saat ini permasalahan keamanan informasi kerap terjadi. Sebagai contoh, terjadi kebocoran informasi pribadi, seperti kartu pengenal, milik seorang pengguna yang merupakan pejabat tinggi negara. Informasi tersebut kemudian diakses oleh pihak yang tidak bertanggung jawab dan

disebarluaskan melalui salah satu situs resmi pemerintah (Alfons, 2021). Data penting dari organisasi perusahaan atau militer, yang seharusnya hanya dapat diakses oleh pihak yang berhak, dapat melibatkan informasi rahasia. Informasi yang bersifat rahasia ini juga bisa berupa gambar, dan digunakan luas dalam berbagai sektor seperti keamanan, medis, seni, dan bidang lainnya (Muhathir, 2018).

Salah satu teknik keamanan informasi yang dapat digunakan adalah kriptografi. Kriptografi adalah teknik untuk melindungi informasi dari pihak yang tidak berwenang. Teknik ini digunakan untuk memastikan privasi, keaslian, dan integritas informasi, bahkan ketika informasi tersebut dikirim melalui saluran yang tidak aman (Coron, 2006). Data yang telah diubah disebut *ciphertext*. Untuk dapat membaca *ciphertext*, diperlukan kunci yang digunakan untuk mengubahnya kembali menjadi bentuk semula, yaitu *plaintext* (Bhanot & Hans, 2015).

Kriptografi dapat digunakan untuk melindungi informasi digital dari penyalahgunaan dengan cara menyembunyikan informasi tersebut dari pihak yang tidak berwenang. Namun, kriptografi saja tidak cukup untuk melindungi informasi digital secara menyeluruh. Hal ini dikarenakan kriptografi hanya melindungi informasi dari penyalahgunaan dengan cara mengubahnya menjadi bentuk yang tidak dapat dibaca.

Metode kriptografi yang akan digunakan pada penelitian ini adalah metode ElGamal. Metode ini dipilih karena keamanan kriptografi ElGamal terletak pada logaritma diskrit pada grup pengandaan bilangan bulat modulo prima, dengan mengambil nilai bilangan prima yang besar (Massandy, 2009). Dengan cara ini, maka metode enkripsi dan dekripsi akan membutuhkan proses komputasi yang besar, sehingga hasil enkripsinya akan berukuran dua kali lebih besar dari ukuran semula (Husaini dkk., 2022).

Salah satu metode dalam melindungi informasi adalah dengan cara menyisipkan pesan di dalam pesan lainnya. Teknik ini, dikenal sebagai steganografi, melibatkan penyembunyian pesan dalam konteks pesan lainnya

guna menghindari kecurigaan terhadap upaya pencurian informasi. Dengan menggunakan teknik ini, pesan rahasia dapat tersembunyi tanpa diketahui oleh pihak lain. Steganografi merupakan seni dan ilmu komunikasi tersembunyi, memiliki kemiripan dengan kriptografi. Dengan steganografi, dua pihak yang saling mempercayai dapat melakukan pertukaran pesan secara rahasia, khususnya dalam konteks steganografi digital yang menggunakan media digital sebagai wadah (Setiawan dkk., 2023).

Steganografi membedakan diri dari kriptografi karena kriptografi berfokus pada memastikan kerahasiaan isi pesan, sedangkan steganografi lebih berorientasi pada menjaga kerahasiaan keberadaan pesan itu sendiri. Jika keberadaan informasi tersembunyi terungkap atau bahkan dicurigai, tujuan steganografi dapat mengalami kegagalan sebagian besar. Oleh karena itu, untuk meningkatkan keamanan steganografi, seringkali dikombinasikan dengan kriptografi (Morkel dkk., 2005).

Salah satu metode persembunyian data/komunikasi tersembunyi yang menggunakan gambar digital sebagai sinyal penyamaran adalah *Spread Spectrum Image Steganography* (SSIS). SSIS memungkinkan penyembunyian dan pemulihan bit informasi dalam jumlah besar di dalam gambar digital dengan bebas kesalahan, tanpa terdeteksi oleh pengamat. SISS memiliki keamanan yang baik karena data disembunyikan melalui proses tambahan melalui XOR sebelum dimasukkan ke dalam gambar sehingga pesan yang disembunyikan dalam gambar lebih sulit dideteksi (Marvel dkk., 1999). Cukup banyak penelitian terdahulu telah menggunakan metode *Spread Spectrum* dan mencatat bahwa hasil pengujian MSE dan PSNR menunjukkan kualitas citra yang baik, dengan nilai PSNR di atas 30 dB.

Karena itu, penelitian ini bertujuan untuk menggunakan algoritma ElGamal dan *Spread Spectrum* untuk menerapkan keamanan berlapis yang akan diimplementasikan untuk sistem pengamanan pesan pada citra.

1.2 Rumusan Masalah

Masalah yang dirumuskan pada penelitian ini adalah bagaimana cara implementasi kombinasi kriptografi ElGamal dan steganografi *Spread Spectrum* dapat meningkatkan keamanan dalam pengiriman pesan rahasia.

1.3 Batasan Masalah

Dari latar belakang proposal serta rumusan masalah yang ada, terdapat beberapa batasan dari lingkup penelitian ini, diantaranya adalah:

1. Penelitian ini menggunakan enkripsi berupa pesan teks dengan tipe TXT.
2. Hasil keluaran yang dihasilkan oleh sistem ini berbentuk citra gambar dengan format PNG.
3. Ukuran bilangan prima yang digunakan pada proses enkripsi dibatasi oleh kemampuan pemrosesan perangkat.
4. Pesan teks yang digunakan adalah UTF-8 dengan set karakter terbatas pada ASCII.

1.4 Tujuan Penelitian

Tujuan utama dari penelitian ini adalah untuk melaksanakan implementasi sistem keamanan pesan pada citra dengan memanfaatkan pesan teks dan mengaplikasikan algoritma kriptografi ElGamal. Selanjutnya, penelitian ini bertujuan untuk memperkuat keamanan dengan menggabungkan metode steganografi *Spread Spectrum*.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian yang dilakukan yaitu dapat menghasilkan sebuah sistem yang dapat mengamankan pesan teks tanpa dicurigai oleh orang lain. Beberapa manfaat yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Bagi pembaca, meningkatkan pemahaman tentang proses penerapan algoritma kriptografi ElGamal dalam konteks pengamanan pesan teks merupakan tujuan utama penelitian ini. Selain itu, penelitian ini juga

bertujuan untuk mendalami pemahaman tentang kontribusi steganografi Spread Spectrum dalam meningkatkan tingkat keamanan pesan teks pada sistem yang dihasilkan.

2. Bagi peneliti, hasil yang diperoleh dari penelitian ini memiliki potensi untuk memberikan kontribusi dalam pengembangan ilmu pengetahuan. Informasi yang dihasilkan dapat berfungsi sebagai rujukan yang berharga dan menjadi landasan penting bagi penelitian-penelitian mendatang yang berkaitan dengan topik yang sama atau serupa.
3. Bagi masyarakat, sistem yang dihasilkan melalui penelitian ini memiliki potensi untuk menjadi sebuah alat yang bermanfaat bagi masyarakat, membantu mereka memahami dengan lebih mendalam tentang kegunaan dan peran keamanan informasi dalam konteks kehidupan sehari-hari. Dengan adanya pemahaman yang lebih baik terkait keamanan informasi, masyarakat dapat meningkatkan kesadaran mereka dan mengambil langkah-langkah yang lebih proaktif dalam melindungi data dan informasi pribadi mereka.

1.6 Sistematis Penelitian

Sistematika penulisan laporan ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Pada bab ini membahas mengenai latar belakang, rumusan masalah, tujuan penelitian, batasan masalah dan manfaat penelitian.

BAB II. TINJAUAN PUSTAKA

Pada bab ini membahas mengenai penelitian terdahulu, landasan teori dan mencakup isi pokok penelitian, tahapan-tahapan dari algoritma kriptografi ElGamal dan steganografi Spread Spectrum.

BAB III. METODOLOGI PENELITIAN

Pada bab ini membahas mengenai jenis dan sumber data penelitian, metode pengumpulan data, metode pengembangan sistem, jenis data yang diperlukan, alat bantu penelitian, kerangka pikir penelitian dan analisis sistem.

BAB VI. HASIL DAN PEMBAHASAN

Bab ini berisi hasil dari penelitian mengenai kombinasi kriptografi ElGamal dan steganografi Spread Spectrum yang dilakukan serta pembahasan mengenai penerapan sistem dalam penelitian ini.

BAB V. PENUTUP

Pada bab ini berisi kesimpulan yang didapatkan dari penelitian beserta saran.