BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Seiring perkembangan teknologi, pesan rahasia semakin mudah diretas oleh pihak yang tidak berwenang. Maka dari itu, perlu adanya upaya untuk meningkatkan keamanan terhadap pesan rahasia. Pesan rahasia dapat diamankan dengan menyamarkan isi pesan. Kemudian dapat ditingkatkan keamanannya dengan menyembunyikan keberadaan pesan tersebut pada suatu media, misalnya gambar.

Kriptografi merupakan ilmu yang mempelajari cara untuk mengamankan pesan dengan menyamarkan isi pesan (Munir, 2019). Dalam kriptografi, terdapat dua proses penting dalam menjaga keamanan data atau informasi, yaitu enkripsi dan dekripsi. Proses enkripsi melibatkan pengubahan pesan asli menjadi bentuk pesan yang tidak dapat dibaca atau tersandi. Melalui proses enkripsi, data menjadi tidak dapat diakses oleh pihak yang tidak berwenang dan hanya dapat dibuka atau dibaca oleh penerima yang memiliki kunci (*key*) yang sesuai. Sementara itu, proses dekripsi berfungsi untuk mengembalikan data yang telah dienkripsi menjadi data asli atau pesan semula (Ulva, 2019). Salah satu algoritma kriptografi yang memberikan solusi untuk permasalahan keamanan informasi adalah algoritma *Affine Cipher*. Algoritma ini termasuk ke dalam kategori *cipher* klasik yang termasuk dalam kriptografi kunci simetris (*symmetric key cryptography*) di mana kunci yang digunakan dalam proses enkripsi dan dekripsi menggunakan kunci yang sama sehingga relatif mudah diretas (Djoko, 2014). Peningkatan keamanan dapat dilakukan dengan menggabungkan dua teknik kriptografi seperti yang dilakukan oleh Fadlan (2017) yang menggabungkan algoritma *Knapsack Merkle Hellman* dan *Affine Cipher*. Selain dengan menggabungkan dua teknik kriptografi, keamanan pesan juga dapat ditingkatkan melalui penggabungan antara teknik kriptografi dan steganografi.

Steganografi mempelajari teknik untuk menyembunyikan keberadaan pesan,

salah satu metode yang umum digunakan adalah *Least Significant Bit* (Munir, 2019). *Least Significant Bit (LSB)* adalah suatu teknik steganografi yang digunakan untuk menyisipkan pesan rahasia ke dalam format yang berbeda (Riski, 2018). Cara kerja metode *Least Significant Bit (LSB)* adalah dengan menyisipkan bit pesan rahasia ke bit terakhir dari setiap elemen citra digital. Selain untuk menyisipkan pesan rahasia ke dalam citra digital, *Least Significant Bit* (LSB) juga dapat digunakan untuk menyembunyikan pesan ke dalam file audio seperti pada penelitian yang dilakukan oleh Humaira (2022). Namun, *Least Significant Bit* (LSB) ini rentan terhadap serangan karena pesan tersembunyi dapat diungkap dengan mengumpulkan bit terakhir. Oleh karena itu perlu dilakukan modifikasi pada metode ini. Adapun salah satu modifikasi *Least Significant Bit* (LSB) adalah *Least Significant Bit-2* (LSB-2). Cara kerja pada metode *Least Significant Bit-2* (LSB-2) ini yaitu dengan menukarkan bit ke 8-2 (bit ke 6) dari setiap elemen warna *pixel* citra digital yang menjadi citra penampung dengan setiap bit pesan rahasia yang akan disembunyikan (Zebua, 2015). Terdapat penelitian yang mengkaji mengenai kombinasi *Least Significant Bit-2* (LSB-2) dengan algoritma *Triangle Chain Cipher* untuk menghasilkan *stegano-image* yang dilakukan oleh Zebua (2015).

Dalam penelitian ini ditelaah penggabungan *Least Significant Bit-2* dan *Affine Cipher* dengan cara menggabungkan kriptografi dan steganografi tersebut. Penggabungan kriptografi dan steganografi ini bertujuan untuk meningkatkan keamanan suatu pesan yang bersifat rahasia sehingga pesan tersebut lebih sulit untuk diretas. Dengan memperhatikan dan menganalisa hal-hal di atas, maka penulis mengadakan penelitian dengan judul: **"Penyisipan Pesan Rahasia pada Gambar dengan Menggunakan *Affine Cipher* dan *Least Significant Bit-2* (LSB-2)".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah diuraikan, terdapat rumusan masalah sebagai berikut:

1. Bagaimana cara melakukan pengamanan pesan menggunakan *Affine Cipher* dan *Least Significant Bit*-2?
2. Bagaimana implementasi algoritma *Affine Cipher* dan *Least Significant Bit-2* dalam bentuk program aplikasi menggunakan bahasa pemrograman Python?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

1. Informasi yang disisipkan berupa file teks dengan karakter ASCII dari 32 sampai 126.
2. File penyisipan informasi yaitu file gambar dengan format .*png.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang sudah diuraikan, terdapat tujuan penelitian sebagai berikut:

1. Mengetahui cara melakukan pengamanan pesan menggunakan penggabungan *Affine Cipher* dan *Least Significant Bit-2*.
2. Memberikan gambaran dari implementasi *Affine Cipher* dan *Least Significant Bit-2* dalam bentuk program aplikasi menggunakan bahasa pemrograman Python.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah:

1. Manfaat Teoritis

   Secara teoritis, penelitian ini dapat berkontribusi dalam mengetahui cara pengamanan pesan teks dengan menggunakan penggabungan algoritma *Affine Cipher* dan *Least Significant Bit-2* (LSB-2).
2. Manfaat Praktis

   Secara praktis, aplikasi yang dikembangkan dengan menggunakan program

Python yang dihasilkan dalam penelitian ini diharapkan dapat memudahkan implementasi pengamanan pesan teks dengan menggunakan kriptografi *Affine Cipher* dan *Least Significant Bit-2* (LSB-2).