# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Seringkali seseorang yang hendak mengirim pesan kepada orang yang dituju, tidak ingin isi pesan tersebut diketahui oleh pihak lain. Umumnya isi pesan tersebut bersifat pribadi atau rahasia yang hanya boleh diketahui antara pihak pengirim dan pihak penerima pesan. Pengirim biasanya mengirim pesan secara rahasia untuk mencegah pihak lain mengetahui

Salah satu teknik yang digunakan untuk keamanan pesan adalah kriptografi. Kriptografi dapat mengubah pesan (*plaintext*) menjadi pesan tersamar (*ciphertex*t), sehingga pesan rahasia hanya dapat dibaca oleh pihak yang berwenang. Ziliwu, Maslan dan Kremer (2022) mengatakan teknik ini dilakukan dengan mengubah teks asli menjadi bentuk yang berbeda atau sering disebut enkripsi. Tujuan utama dari kriptografi adalah melindungi kerahasiaan isi pesan dengan membuatnya sekompleks mungkin sehingga sulit dipecahkan tanpa kunci yang tepat.

Tambahan teknik yang dapat digunakan untuk keamanan pesan adalah steganografi. Steganografi merupakan teknik untuk menyembunyikan (*embedding*) pesan ke dalam media digital. Media digital yang digunakan dalam steganografi ini adalah teks, gambar, suara dan video (Bharti dkk., 2019). Dengan menggunakan steganografi, informasi rahasia dapat disimpan secara terselubung dalam media seperti teks, gambar digital, suara, dan video, sehingga tidak dapat dideteksi oleh pihak lain dan memastikan privasi informasi tersebut.

Dengan ditambahnya teknik steganografi, teknik tersebut dapat melindungi sebuah pesan akan tetapi tidak menjamin sebuah pesan aman, dalam mengatasi permasalahan tersebut, penelitian ini akan menggunakan kombinasi kriptografi dan steganografi untuk keamanan pesan sehingga menghasilkan sistem keamanan yang aman. Biasanya teknik pertama yaitu mengenkripsi pesan terlebih dahulu pada proses kriptografi, kemudian menyisipkannya ke media *cover* yang disebut steganografi.

Banyaknya metode dalam melindungi keamanan data pada kriptografi, maka dipilihlah teknik kriptografi Vigènere *cipher*. Vigènere *cipher* merupakan bagian dari awal perkembangan ilmu kriptografi, atau bagian dari kriptografi klasik. Namun seiring dengan perkembangan ilmu pengetahuan manusia, kelemahan dari Vigènere *cipher* berhasil ditemukan. Salah satu kelemahan dari Vigènere *cipher* ini adalah kuncinya yang berulang sehingga dapat ditebak dengan tepat (Hikmah, 2020). Salah satu cara yang dapat dilakukan untuk mengatasi kelemahan Vigènere *cipher* tersebut adalah dengan melakukan pembangkitan kunci yang lebih acak (Mulyadi, 2018). Kunci yang dibangkitkan secara acak tahan terhadap serangan analisa frekuensi tinggi (Ndruru dan Zebua, 2022). Algoritma Vigènere *cipher* memanfaatkan substitusi polialfabetik yang ada pada data atau pesan yang akan diamankan dengan menggunakan sebuah kunci berupa jumlah pergeseran dan kata atau susunan kata untuk proses pengacakan data atau pesan. Proses yang dilakukan yaitu adalah enkripsi dan dekripsi (Zuli dan Irawan, 2014).

Vigènere *cipher* adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso (Munir, 2019). Beliau menuliskan metodenya tersebut pada bukunya yang berjudul *La Cifra del. Sig. Giovan Battista Bellaso* pada tahun 1553. Nama Vigènere sendiri diambil dari seorang yang bernama Blaise de Vigenère. Nama Vigènere diambil sebagai nama algoritma ini karena beliau menemukan kunci yang lebih kuat (Munir, 2019).

Dalam konteks steganografi, salah satu media yang umum digunakan sebagai *cover* untuk menyembunyikan informasi rahasia adalah berkas gambar. Menurut Susanto dan Yusnaini (2019), Penggunaan teknik steganografi pada berkas gambar didasarkan pada kelemahan persepsi visual manusia, di mana perbedaan kualitas antara gambar asli dan gambar yang telah mengandung data rahasia tidak secara signifikan terlihat oleh mata manusia. Dalam konteks ini, terdapat beragam teknik yang telah dikembangkan untuk menyembunyikan dan menyisipkan data dalam media *cover*. Salah satu teknik yang sering digunakan adalah metode *Least Significant Bit* (LSB).

Pada tahun 2018, dilakukan penelitian Septa Festi Burna Jaya, Susanti M. Kuway dan Gusti Syarifudin dengan judul "Perancangan Perangkat Lunak

Steganografi Menggunakan *Least Significant Bit* Dengan Enkripsi Vigènere *Cipher*". Tujuan penelitian ini adalah untuk meningkatkan keamanan metode *Least Significant Bit* (LSB) yang digunakan dalam steganografi dengan menggabungkannya dengan teknik kriptografi simetris Vigènere. Metode LSB dalam steganografi digunakan untuk menyembunyikan data rahasia dalam media cover. Namun, metode ini memiliki kelemahan jika LSB digunakan secara sekuensial, karena dapat mudah dideteksi oleh pihak yang tidak berwenang (Lubis, 2020). Sehingga, penulis tertarik untuk meneliti bentuk lain dari algoritma sekuential yaitu menggunakan algoritma *Blum Blum Shub.* Naufal (2020) mengemukakan dalam penelitiannya algoritma *Blum Blum Shub* dapat meningkatkan keamanan algoritma Affine *Cipher* dengan memanfaatkan barisan bilangan acak yang tidak dapat diprediksinya

Dengan demikian penulis mengkaji penelitian dengan judul "Implementasi Steganografi Kombinasi *Least Significant Bit* dan *Blum Blum Shub* Dengan Kriptografi Vigènere *Cipher* Untuk Penyisipan 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 melakukan proses enkripsi dan dekripsi menggunakan metode kriptografi Vigènere serta menggabungkannya dengan metode steganografi gambar menggunakan LSB acak?
2. Bagaimana konstruksi program aplikasi kriptografi Vigènere dengan metode steganografi LSB acak?

## 1.3 Batasan Masalah

Batasan masalah yang digunakan pada penelitian ini adalah:

1. Pesan yang tersembunyi dalam konteks ini merujuk pada pesan teks yang terdiri dari karakter ASCII yang muncul dari karakter ke-32 hingga karakter ke-126. Hal ini disebabkan oleh penggunaan karakter-karakter tersebut dalam konteks penulisan secara umum.
2. Cover media yang digunakan dalam penelitian ini adalah gambar berwarna *Red, Green,* dan *Blue (RGB)* dengan format *file* .png.

3. Pesan yang digunakan dalam penelitian ini berformat .txt
4. Memiliki batasan panjang pesan

## 1.4 Tujuan Penelitian

Adapun tujuan penelitian ini antara lain:

1. Mengimplimentasikan algoritma kriptografi Vigènere pada Steganografi gambar dikombinasikan dengan metode *Least Significant Bit* LSB
2. Mengimplementasikan penggabungan algoritma kriptografi Vigènere dan steganografi dengan metode *Least Significant Bit* (LSB) dalam pengembangan program komputer menggunakan bahasa pemrograman *Python*

## 1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan pada penelitian ini antara lain:

1. Menerapkan dan mengembangkan ilmu pengetahuan tentang metode kriptografi dikombinasi dengan steganografi.
2. Membantu mengamankan informasi yang bersifat rahasia dan mempersulit orang yang tidak bertanggung jawab dalam mengambil data tersebut

## 1.6 Sistematika Penulisan

Sistematika penulisan penelitian ini sebagai berikut:

1. **BAB I PENDAHULUAN**

   Bab ini menjelaskan mengenai latar belakang penelitian, rumusan masalah, tujuan penelitian dan manfaat penelitian.

2. **BAB II KAJIAN TEORI**

   Bab ini mengandung teori dasar dan konsep-konsep mengenai kriptografi Vigènere dan dan steganografi yang dikaji dari beberapa sumber literatur yang menunjang penelitian.

3. **BAB III METODOLOGI PENELITIAN**

   Bab ini menjelaskan mengenai model dasar dan langkah-langkah yang digunakan dalam menyelesaikan penelitian

4. **BAB IV HASIL DAN PEMBAHASAN**

Bab ini membahas mengenai hasil penelitian yang telah dilakukan dan menjelaskan konstruksi program yang telah dibuat.

5. **BAB V KESIMPULAN DAN SARAN**

   Bab ini memberikan kesimpulan hasil penelitian dan saran-saran untuk penelitian selanjutnya.