BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan telekomunikasi semakin pesat membuat kegiatan manusia semakin mudah, diantaranya mengirim informasi dengan cepat. Kemajuan teknologi dalam megiriman informasi masih terdapat bahaya penyalahgunaan informasi. Salah satu dari dampak tersebut yaitu dapat diretasnya informasi bersifat pribadi yang dapat disalahgunakan oleh pihak yang tidak bertanggungjawab, misalkan pada kasus "Peretasan WhatsApp Direktur Utama PT Tempo Inti Media Tbk, Toriq Hadad (Velarosdela, 2019). Untuk mencegah hal tersebut, diperlukan suatu pengamanan informasi pada pesan teks.

Terdapat beberapa cara untuk pengamanan pesan tersebut, diantaranya dengan kriptografi dan steganografi. Steganografi sering dikaitkan dengan kriptografi namun kedua metode ini sangatlah berbeda. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Ariyus, 2008). Untuk keamanan pesan tersebut dibutuhkan proses penyandian, yakni proses yang akan mengubah *plaintext* (pesan asli) menjadi *ciphertext* (pesan tersamar) yang dapat dibuka oleh penerima yang memiliki kunci. Algoritma kriptografi yang digunakan penulis yaitu *Advanced Encryption Standard* (AES). AES atau sering disebut Rijndael ini merupakan standard kriptografi yang ditetapkan *National Institute of Standards and Technology* (NIST) sebagai pengganti DES karena algoritma DES mempunyai kelemahan yang cukup fatal. Sehingga pada bulan Oktober 2000, NIST menetapkan AES sebagai algoritma standard kriptografi yang masih bertahan hingga saat ini (Munir, 2007). Pabokory, dkk (2015) menyimpulkan bahwa AES terbukti sulit menghadapi serangan yang menggunakan statistik untuk memecahkan sandi, karena dalam enkripsi dan dekripsi harus melakukan 10 putaran dalam melakukan pengamanan maupun untuk membuka pengamanan

tersebut. Bagaimanapun ditemukannya pesan yang telah disamarkan oleh pihak yang tidak bertanggungjawab akan menimbulkan kecurigaan sehingga aksi peretasan pun dapat dilakukan. Atas dasar hal tersebut perlu adanya upaya untuk menyembunyikan *ciphertext* hasil kriptografi AES, maka dilakukan steganografi supaya pihak yang tidak bertanggungjawab tidak mengetahui adanya pesan yang dikirim.

Steganografi merupakan teknik menyembunyikan informasi ke dalam sebuah media, bisa berupa media gambar, suara maupun video sehingga pesan rahasia tersebut tidak dapat diketahui keberadaannya oleh orang lain, dan media yang cukup sering digunakan sebagai *cover* yaitu media gambar (citra digital). Citra digital sering digunakan sebagai media untuk menyembunyikan pesan tersembunyi. Menurut Batarius dan Maslim (2012), dalam steganografi terdapat beberapa metode, yaitu *Least Significant Bit* (LSB), *Discrete Cosine Transform* (DCT), *Discrete Wavelete Transform* (DWT), dan *PeakSignal To Noise Ratio* (PSNR). Metode yang sederhana dari steganografi yang digunakan penulis yaitu steganografi *Least Significant Bit* (LSB), dan metode LSB yang digunakan adalah LSB terurut, karena dilakukan dengan dengan mengganti bit terakhir dari setiap *pixel* pada gambar dan menggantikannya dengan bit pesan yang akan disembunyikan. A.Mufadilah, (2019) dalam skripsinya menyebutkan bahwa hasil akhir metode steganografi LSB tidak akan jauh berbeda dengan gambar yang belum disisipkan pesan, bahkan tidak terlihat perbedaanya secara kasat mata.

Berdasarkan penjelasan di atas, penulis tertarik untuk untuk mengkaji penggabungan kriptografi AES dengan steganografi LSB untuk meningkatkan keamanan pesan. Kemudian dari kombinasi tersebut akan dibuat program menggunakan bahasa pemograman Python. Oleh karena itu, penulis mengambil judul "Pengamanan Pesan Teks dengan Kriptografi *Advanced Encryption Standard* (AES) dan Steganografi *Least Significant Bit* (LSB)".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah, maka perumusan masalah yang diambil yaitu:

1. Bagaimana prosedur penggabungan algoritma kriptografi AES dan steganografi LSB?
2. Bagaimana implementasi penggabungan algoritma kriptografi AES dan steganografi LSB dalam bentuk program dengan bahasa pemrograman Python?

1.3 Tujuan Masalah

Tujuan dalam penelitian ini adalah sebagai berikut:

1. Memperoleh gabungan algoritma dari kriptografi AES dan steganografi LSB.
2. Memberikan gambaran dari implementasi penggabungan algoritma kriptografi AES dan steganografi LSB dalam bentuk program dengan bahasa pemrograman Python.

1.4 Batasan Masalah

Adapun pembatasan masalah dalam penelitian ini adalah sebagai berikut.

1. Kriptografi AES yang digunakan berupa AES-128.
2. Media gambar yang digunakan yaitu gambar berwarna dengan format *JPG.
3. Metode steganografi yang digunakan adalah LSB secara terurut.

1.5 Manfaat Masalah

Adapun manfaat yang diharapkan dari penelitian ini adalah:

1. Dapat meningkatkan pemahaman mengenai kriptografi AES dan Steganografi metode LSB pada pengamanan pesan teks, dan digunakan sebagai tambahan pemahaman untuk bahan kajian dan referensi untuk penelitian kriptografi AES dan Steganografi metode LSB lainnya.
2. Dapat memberi kontribusi dalam bidang matematika terapan dalam pengembangan kriptografi AES dan Steganografi LSB dalam bentuk program aplikasi komputer dengan bahasa pemrograman Python 3.7.

1.6 Sistematika Penelitian

Penulisan skripsi ini akan dibagi menjadi beberapa bab, yaitu:

a. BAB I PENDAHULUAN

   Bab ini terdiri atas latar belakang, rumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika penulisan.

b. BAB II LANDASAN TEORI

   Pada bab ini akan dijabarkan konsep dasar Kriptografi AES dan Steganografi dengan metode LSB.

c. BAB III METODE PENELITIAN

   Bab ini berisi mengenai langkah-langkah penulis dalam melaksanakan penelitian.

d. BAB IV PEMBAHASAN

   Pada bab ini dibahas mengenai hasil penelitian yang telah diperoleh.

e. BAB V KESIMPULAN DAN SARAN

   Pada bab ini dijelaskan kesimpulan dari hasil penelitian dan diberikan saran untuk pembaca.