BAB I
PENDAHULUAN

1.1 Latar Belakang

Citra atau gambar digital adalah satu dari banyak jenis data yang digunakan orang-orang saat ini dalam komunikasi melalui media internet. Evolusi pengunaan media sosial telah memfasilitasi berbagai jenis informasi baik teks, gambar, audio dan video. Di sisi lain, perkembangan tersebut memudahkan pihak-pihak tertentu untuk melakukan kecurangan terhadap data atau informasi yang didistribusikan, seperti penyadapan informasi, pemantauan informasi, dan pemalsuan informasi atau penggunaan informasi tersebut untuk kepentingan tertentu (Zebua dan Ndruru, 2017). Gambar atau citra digital sangat informatif membedakannya dari teks. Media informasi berupa media gambar mempunyai kelemahan yaitu mudah dimanipulasi oleh pihak-pihak yang memiliki kepentingan lainnya di dalamnya. Apalagi jika informasi yang terdapat dalam file gambar tersebut mengandung informasi sensitif. Data pribadi, dokumen pemerintahan, atau data medis rumah sakit. (Rakhman dan Kurniawan, 2018).

Salah satu cara untuk mengamankan data dengan melakukan proses penyandian terhadap data yang ingin diamankan sehingga makna sebenarnya dari data tidak dapat dimengerti merupakan teknik kriptografi. Pada umumnya, Teknik kriptografi ada dua algoritma yaitu enkripsi dan dekripsi. *Plaintext* adalah pesan yang dapat dibaca, tetapi proses untuk membuat pesan tidak dapat dibaca disebut enkripsi. *Ciphertext* adalah jenis pesan yang telah melalui proses enkripsi, dekripsi adalah cara mengubah ciphertext menjadi plaintext, dan kunci *key* adalah kode yang digunakan untuk mengenkripsi atau mendekripsi teks (Supriyanto dan

Ardhianto, 2008). Saat menyandikan pesan, ada dua jenis algoritma berbasis kunci, yaitu algoritma Simetris (Konvensional) dan algoritma asimetris (Kunci-publik). Kriptografi Hill adalah kriptosistem kunci simetris yang dapat digunakan untuk melindungi data dengan melakukan proses enkripsi terhadap objek yang ingin diamankan. RSA merupakan *Public-Key Cryptosystem* didalam *public key cryptosystem* ada dua kunci berbeda *public key* yang diketahui publik dan *secret key* atau kunci pribadi yang dirahasiakan pemiliknya. Sistem ini disebut Asimetriks karena kunci yang digunakan untuk enkripsi dan dekripsi – kunci publik dan kunci pribadi.

Hill Cipher merupakan kriptografi kunci simetrik, didalam jenis kriptografi ini pengirim dan penerima mengetahui kunci *secret key* yang sama. Dalam kriptografi simetrik kunci memegang peran yang sangat penting. Sementara RSA merupakan kriptografi Asimetrik dengan *public key cryptosystem* kunci berfungsi berpasangan dengan kunci publik dan pribadi yang cocok. Teknik kriptografi Asimetrik ini membutuhkan beberapa algoritma untuk mengenkripsi data.

Pada penelitian ini *Hill Cipher* akan dikombinasikan dengan RSA untuk melakukan enkripsi terhadap citra, sehingga mampu menyembunyikan informasi yang tersimpan dalam citra tersebut agar tidak diketahui oleh pihak-pihak yang tidak memiliki kepentingan didalamnya.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, pertanyaan dalam penelitian ini adalah bagaimana mengimplementasikan kombinasi algoritma *Hill* dan *Rivest Shamir Adleman* (RSA) dalam proses enkripsi dan dekripsi citra.

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah :

1. Dapat melakukan enkripsi file citra menggunakan kombinasi *hill cipher* dan RSA.
2. Dapat mengamankan informasi dari sebuah citra agar tidak dapat dimengerti dengan kasat mata.

1.4 Batasan Masalah

Adapun batasan masalah pada penelitian ini yaitu :

1. File yang digunakan adalah citra digital berformat .jpg atau .png.
2. File yang digunakan adalah citra keabuan atau grayscale Lena, Cameraman, Enstein, Smadrill/Baboon.
3. Ukuran maksimal citra 512x512 *pixel*.
4. Bahasa pemrograman yang digunakan adalah *Python*.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini antara lain :

1. Sebagai usaha mengamankan sebuah informasi penting dimana hanya orang tertentu saja yang berhak mengetahuinya.
2. Menambah literatur dan rujukan dalam bidang ilmu kriptografi mengenai pengamanan terhadap file citra menggunakan kombinasi algoritma *Hill cipher* dan *Rivest Shamir Adleman* (RSA).