BAB I
PENDAHULUAN

1.1 Latar Belakang

Kasus kebocoran data di era digital menjadi pengingat bahwa keamanan data digital sangat penting. Dikutip dari CNN Indonesia (2022), data masyarakat yang diduga bocor dari Kementerian Sosial (Kemensos) dijual di *dark web* pada 2022. Data yang bocor diantaranya foto Kartu Tanda Penduduk (KTP) dan Kartu Keluarga (KK) (CNN Indonesia, 2022). Menurut Kamal dkk. (2021), jika pesan pada gambar tersebut dapat digunakan secara tidak sah, hal ini akan menimbulkan masalah yang serius. Pesan pada gambar dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, gambar perlu diamankan sehingga pesan pada gambar tidak dapat diketahui.

Seni dan ilmu menjaga keamanan pesan disebut kriptografi (Schneier, 1995). Kriptografi adalah seni mencapai keamanan dengan cara menyandikan pesan ke dalam bentuk yang tidak dapat dibaca (Kahate, 2013). Proses meyandikan pesan ini disebut enkripsi (Kahate, 2013). Pesan yang telah disandikan dapat dikembalikan menjadi pesan semula. Proses ini disebut dekripsi (Kahate, 2013). Enkripsi dan dekripsi ini dilakukan menggunakan kunci (Kahate, 2013).

Menurut Nahar & Chakraborty (2020), *rail-fence cipher* adalah algoritma kriptografi yang paling sederhana dan menarik dari banyak algoritma kriptografi yang telah dikembangkan. Algoritma ini menyandikan pesan dengan cara mengubah urutan elemen pada pesan. Namun, algoritma ini memiliki masalah, yaitu pesan yang dienkripsi dapat diungkap dengan mudah (Shaker, dkk., 2022).

Menurut Shaker dkk. (2022), *Advanced Encryption Standard* (AES) adalah algoritma kriptografi terkuat. AES yang dipublikasikan oleh National Institute of Standards and Technology (Stallings, 2023; NIST, 2023) tidak dapat dibobol secara paksa, bahkan dengan kekuatan komputasi saat ini (Shaker, dkk., 2022). Selain itu, AES merupakan algoritma kriptografi yang digunakan secara luas (Blazhevski, dkk., 2013). Oleh karena itu, Shaker dkk. (2022) mengusulkan kombinasi antara AES dan *rail-fence cipher* untuk mengatasi masalah *rail-fence cipher*. Kombinasi ini disebut RAES. Shaker dkk. (2022) menerapkan RAES ini pada pesan berupa teks menggunakan kunci berukuran 128-bit (RAES-128), 192-bit (RAES-192), dan

256-bit (RAES-256). AES dan RAES ini termasuk ke dalam *block cipher*, yaitu algoritma kriptografi yang memproses pesan berbentuk blok.

NIST mendefinsikan lima mode operasi untuk menerapakan *block cipher* (Dworkin, 2001; Stallings, 2023). Berdasarkan lima mode operasi tersebut, Blazhevski dkk. (2013) memilih mode operasi *Counter* untuk menerapkan AES dengan tepat dan aman. Kelebihan mode operasi ini adalah *block cipher* dapat diterapkan tanpa pesan tambahan (Blazhevski dkk., 2013).

Godara dkk. (2018) mengusulkan pendekatan lain untuk mengatasi kelemahan pada keamanan *rail-fence cipher*, yaitu *block rail-fence cipher*. Algoritma ini mengenkripsi pesan sebagai blok-blok dengan panjang yang berbeda menggunakan *rail-fence cipher* yang telah dioptimalkan. Selain itu, kunci yang digunakan pada algoritma ini adalah kunci yang telah dikelola.

RAES yang dikembangkan Shaker dkk. (2022) perlu dimodifikasi. Shaker dkk. (2022) tidak menjelaskan cara menangani kunci 0 yang terdefinisi di RAES, tapi tidak dapat digunakan pada *rail-fence cipher* karena kunci *rail-fence cipher* harus bernilai lebih dari 0. Godara dkk. (2018) menginspirasi penelitian ini untuk melakukan modifikasi berupa pengelolaan kunci *rail-fence cipher* di RAES sehingga semua kunci di RAES dapat digunakan pada *rail-fence cipher* RAES. Selain itu, modifikasi ini dilakukan untuk menyamarkan kunci yang sebenarnya digunakan. Berdasarkan Godara dkk. (2018) juga, modifikasi lain dilakukan pada RAES, yaitu menggunakan *rail-fence cipher* yang dioptimalkan pada RAES agar RAES dapat berjalan lebih efisien.

Pada penelitian ini, RAES yang dimodifikasi akan diterapkan ke dalam bentuk pesan yang lain, yaitu gambar. Berdasarkan Blazhevski dkk. (2013), kelebihan dari mode operasi *Counter* membuat mode operasi ini menjadi pilihan yang tepat untuk menerapkan RAES pada gambar. Pada mode operasi ini, *counter* awal perlu dipilih. Pemilihan *counter* awal ini akan lebih baik jika dapat dilakukan secara otomatis. Pada penelitian ini, *counter* awal akan dipilih secara otomatis berdasarkan kunci dengan tetap menjaga kerahasiaan kunci yang digunakan. Oleh karena itu, penelitian ini mengambil judul "Kriptografi Gambar Menggunakan Mode Operasi *Counter* RAES yang Dimodifikasi".

1.2 Rumusan Masalah

Rumusan masalah pada penelitian ini sebagai berikut.

1. Bagaimana proses kriptografi gambar menggunakan mode operasi *Counter* RAES yang dimodifikasi?
2. Bagaimana konstruksi program aplikasi kriptografi gambar menggunakan mode operasi *Counter* RAES yang dimodifikasi?

1.3 Batasan Masalah

Batasan masalah penelitian ini sebagai berikut.

1. Algoritma kriptografi yang digunakan adalah RAES-128, RAES-192, dan RAES-256 dalam mode operasi *Counter*.
2. Gambar yang digunakan adalah gambar RGB 8-bit.
3. Format yang digunakan untuk masukan gambar adalah *.jpg, *.jpeg, *.png, dan *.bmp.
4. Format yang digunakan untuk keluaran gambar adalah *.png dan *.bmp.
5. Program aplikasi dikonstruksi menggunakan Python.

1.4 Tujuan Penelitian

Tujuan penelitian ini sebagai berikut.

1. Mengimplementasikan kriptografi gambar menggunakan mode operasi *Counter* RAES yang dimodifikasi.
2. Mengonstruksi program aplikasi kriptografi gambar menggunakan mode operasi *Counter* RAES yang dimodifikasi.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini sebagai berikut.

1. Penelitian ini diharapkan dapat memberikan sumbangan pemikiran dalam memperkaya wawasan tentang kriptografi, yaitu kriptografi gambar menggunakan mode operasi *Counter* RAES yang dimodifikasi.
2. Penelitian ini diharapkan dapat bermanfaat karena penelitian ini mengembangkan program aplikasi untuk membantu mengimplementasikan kriptografi gambar menggunakan mode operasi *Counter* RAES yang dimodifikasi.