# BAB III
# METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah studi literatur, pengembangan model kriptosistem, dan pengujian model menggunakan program aplikasi. Langkah-langkah penelitian diuraikan sebagai berikut.

## 3.1 Identifikasi Masalah

Penelitian ini menggunakan RAES yang dimodifikasi dalam mode operasi *Counter* pada pesan berupa gambar untuk menghadirkan keamanan berupa *confidentiality* (kerahasiaan). RAES ini memiliki tiga pilihan kunci, yaitu kunci berukuran 128-bit, 192-bit, dan 256-bit. Gambar yang digunakan adalah gambar RGB 8-bit. Hal ini berarti elemen pada gambar dapat dinyatakan sebagai *byte*. *Byte* ini merupakan salah satu bentuk representasi elemen $GF(2^8)$. Hal ini sesuai dengan RAES yang elemennya adalah elemen $GF(2^8)$. Oleh karena itu, kriptosistem pada penelitian ini didefinsikan sebagai lima tupel $(\boldsymbol{\mathcal{P}}, \boldsymbol{\mathcal{C}}, \boldsymbol{\mathcal{K}}, \boldsymbol{\mathcal{E}}, \boldsymbol{\mathfrak{D}})$ sebagai berikut.

- $\boldsymbol{\mathcal{P}} = GF(2^8)$ adalah himpunan berhingga dari kemungkinan *plaintext*.
- $\boldsymbol{\mathcal{C}} = GF(2^8)$ adalah himpunan berhingga dari kemungkinan *ciphertext*.
- $\boldsymbol{\mathcal{K}} = GF(2^8)$ adalah himpunan berhingga kunci yang mungkin (ruang kunci).
- $\boldsymbol{\mathcal{E}} = \boldsymbol{\mathfrak{D}} = \{RAES\text{-CTR-}128, RAES\text{-CTR-}192, RAES\text{-CTR-}256\}$ adalah himpunan berhingga aturan enkripsi dan dekripsi, di mana RAES-CTR-128, RAES-CTR-192, dan RAES-CTR-256 adalah algoritma enkripsi sekaligus dekripsi RAES dalam mode operasi *Counter* dengan kunci masing-masing berukuran 128-bit, 192-bit, dan 256-bit.

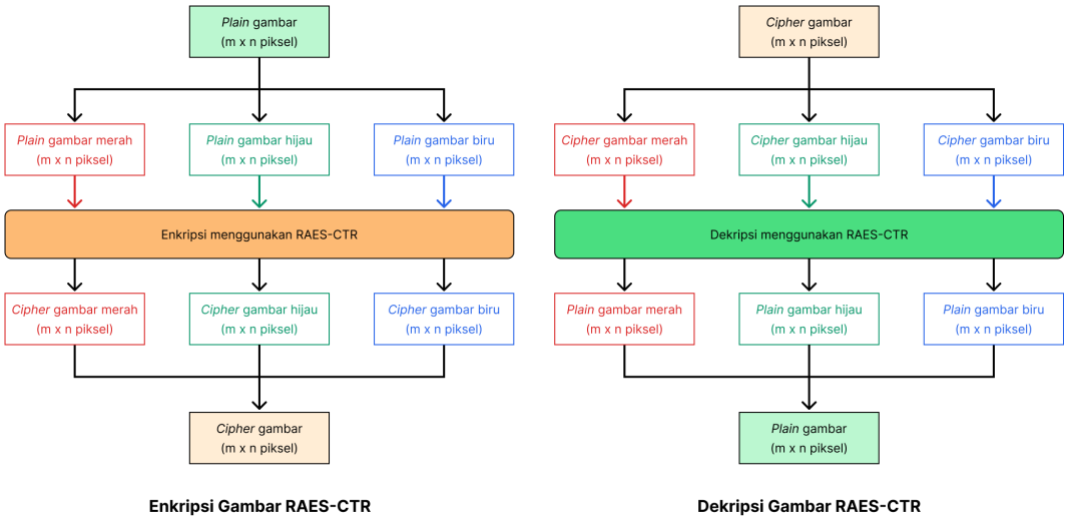
## 3.2 Model Dasar

Model dasar yang digunakan pada penelitian ini adalah enkripsi RAES, enkripsi *rail-fence cipher*, mode operasi *Counter*, dan kriptografi gambar. Model dasar enkripsi RAES dijelaskan pada 2.4. Model dasar enkripsi *rail-fence cipher* dijelaskan pada 2.2.7. Model dasar mode operasi *Counter* dijelaskan pada 2.2.10. Model dasar kriptografi gambar dijelaskan pada 2.2.3.

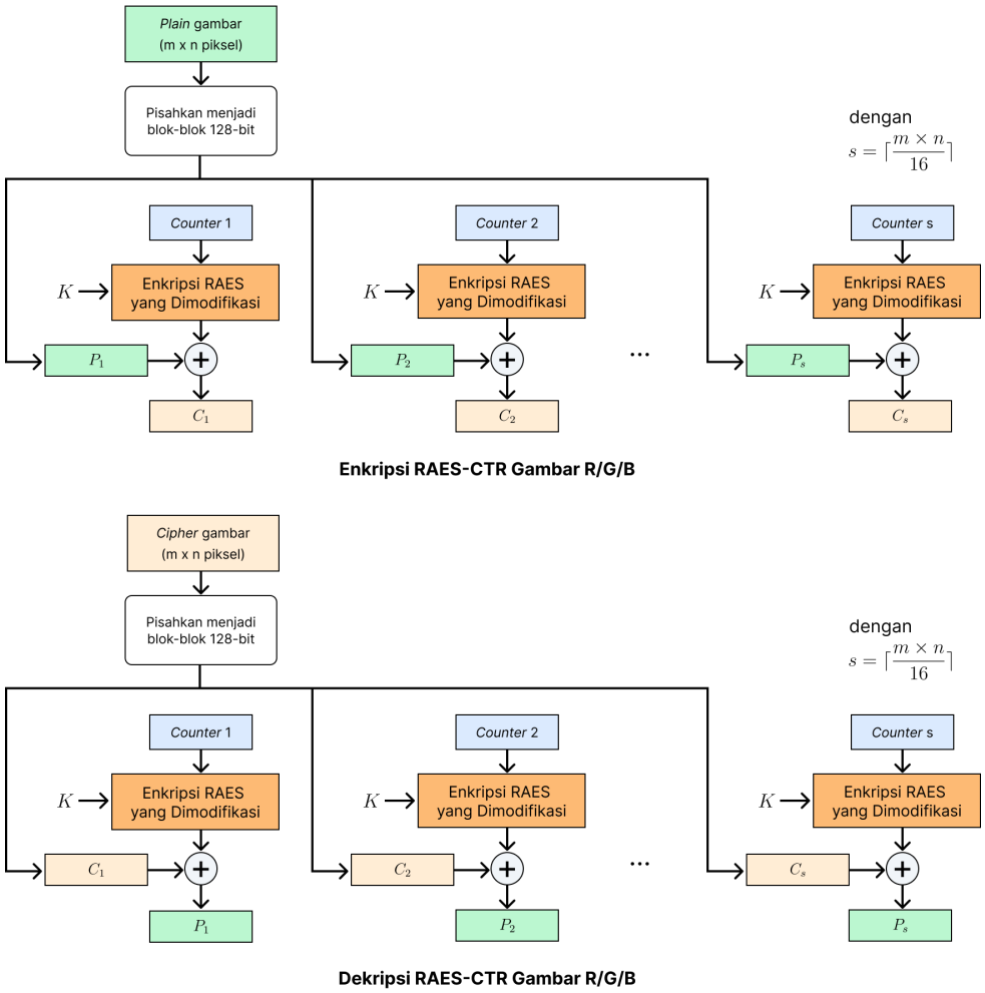
## 3.3 Pengembangan Model Dasar

Pada penelitian ini, model dasar kriptografi gambar dikembangkan dengan menerapkan RAES yang dimodifikasi dalam mode operasi *Counter* (RAES-CTR) sebagai algoritma kriptografi. Hal ini diilustrasikan pada Gambar 3.1. Pada mode

operasi *Counter*, gambar ini perlu dipartisi menjadi blok-blok berukuran 128-bit seperti pada Gambar 3.2.

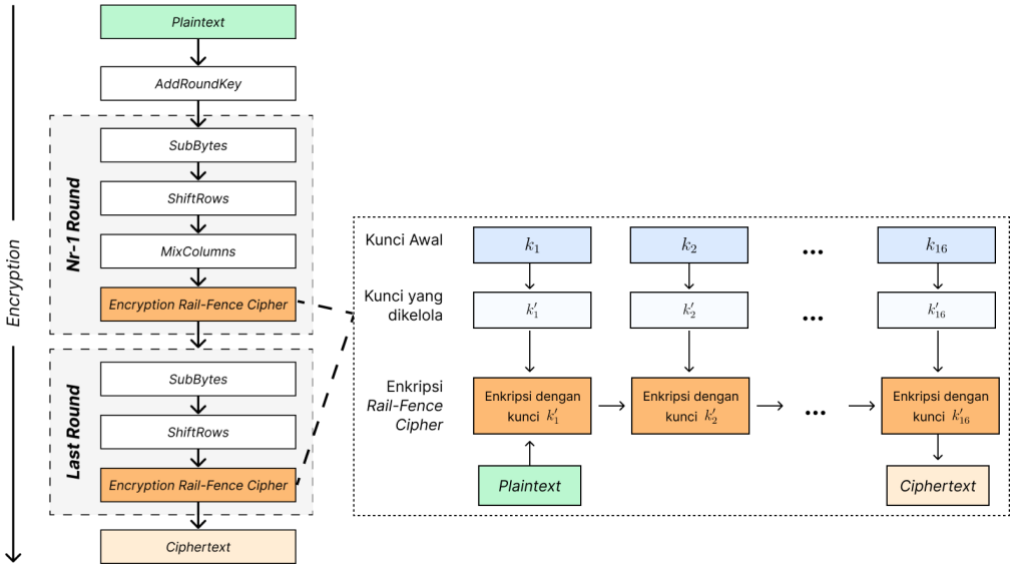



Gambar 3.1 Enkripsi dan Dekripsi Gambar dengan RAES-CTR




Gambar 3.2 Enkripsi dan Dekripsi Komponen Gambar Merah, Hijau, dan Biru dengan RAES-CTR

Pada RAES-CTR, enkripsi dan dekripsi dilakukan dengan hanya melibatkan algoritma enkripsi RAES seperti pada Gambar 3.2. Modifikasi dilakukan pada algoritma dan kunci *rail-fence cipher* yang akan digunakan. Algoritma enkripsi *rail-fence cipher* yang akan digunakan adalah algoritma yang telah dioptimalkan seperti yang dijelaskan pada 2.3. *Rail-fence cipher* diterapkan secara berulang menggunakan kunci yang bersesuaian. Kunci yang digunakan pada *rail-fence cipher* ini adalah kunci yang dikelola terlebih dahulu dengan aturan tertentu. Enkripsi *rail-fence cipher* ini diilustrasikan pada Gambar 3.3. Pada penelitian ini, *counter* dibangkitkan berdasarkan contoh pembangkitan *counter* yang dibahas pada 2.2.10. Pembangkitan *counter* ini akan disesuaikan agar dapat dilakukan tanpa harus berurutan.




Gambar 3.3 Modifikasi enkripsi *rail-fence cipher* pada RAES

## 3.4 Konstruksi Program Aplikasi

Program aplikasi dibangun menggunakan bahasa pemrograman Python. Rincian terkait program aplikasi ini sebagai berikut.

### 3.4.1 Masukan dan Keluaran

Masukan program aplikasi adalah gambar dan sebuah kunci. Masukkan gambar adalah gambar RGB. Pembeda antara enkripsi dan dekripsi hanya terletak pada masukan gambar ini. Masukan kunci adalah teks berisi kumpulan bilangan bulat bernilai 0 hingga 255 yang dipisahkan dengan koma. Keluaran program aplikasi ini adalah gambar yang telah dienkripsi atau didekripsi.

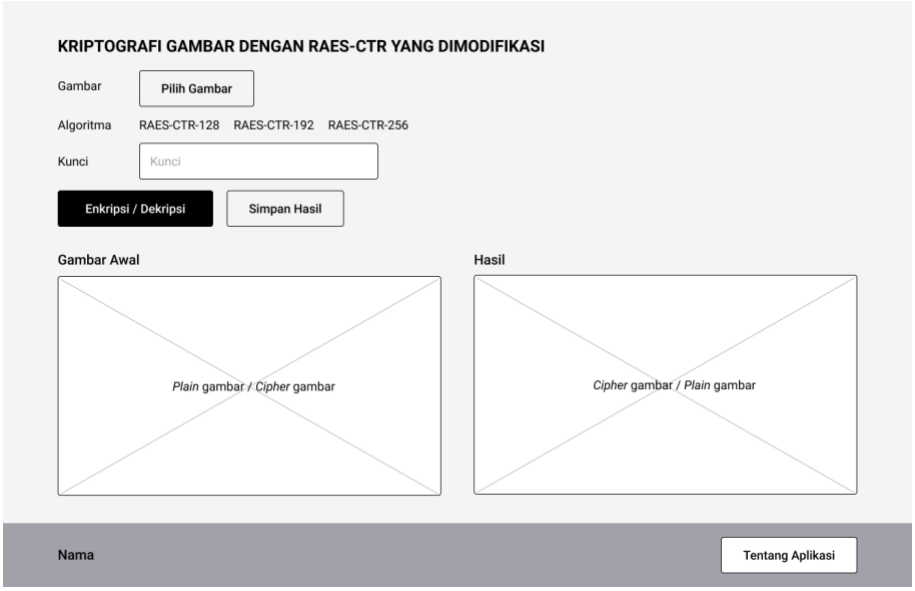
### 3.4.2 Algoritma Deskriptif

Enkripsi dan dekripsi menggunakan RAES-CTR pada penelitian ini dilakukan sebagai berikut.

1. Pengguna memilih gambar yang akan dienkripsi atau didekripsi.
2. Pengguna memilih algoritma yang digunakan, yaitu RAES-CTR-128, RAES-CTR-192, dan RAES-CTR-256
3. Pengguna memasukkan sebuah kunci berupa kumpulan bilangan bulat bernilai 0 hingga 255 yang dipisahkan dengan koma.
4. Pengguna menekan tombol **Enkripsi / Dekripsi** untuk melakukan enkripsi atau dekripsi gambar
5. Pengguna menyimpan gambar yang telah dienkripsi atau didekripsi

### 3.4.3 Rancangan Tampilan

Rancangan tampilan dari program aplikasi disajikan sebagai berikut.




Gambar 3.4 Rancangan Tampilan Program Aplikasi

### 3.4.4 *Library*

*Library* pada Python digunakan untuk memudahkan pembuatan program aplikasi pada penelitian ini. *Library* yang digunakan pada penelitian ini sebagai berikut.

1. CustomTkinter

CustomTkinter adalah *library* tambahan tampilan pengguna pada Python yang dibuat berdasarkan Tkinter. Tkinter adalah *library* standar pada Python yang

digunakan untuk membangun GUI (*Grafical User Interface*) atau antarmuka grafis pengguna. CustomTkinter dapat digunakan sama seperti Tkinter atau dapat dikombinasikan dengan Tkinter. CustomTkinter menyediakan fitur baru yang mebuat proses pembangunan tampilan pengguna lebih mudah.

2. PIL (*Python Imaging Library*)

PIL adalah *library* tambahan pada Python yang digunakan untuk mengelola gambar. PIL digunakan untuk membuka, memanipulasi, dan meyimpan banyak format gambar yang berbeda.

3. Numpy

Numpy adalah *library* tambahan pada Python yang digunakan untuk mengelola larik. Numpy membuat pengelolaan larik menjadi lebih mudah dan lebih cepat. Pengelolaan larik ini termasuk operasi matematika, dasar aljabar linier, dan operasi statistika dasar.

4. Numba

Numba adalah *library* tambahan pada Python yang digunakan untuk mempercepat eksekusi kode Python. Numba bekerja dengan cara menerjemahkan fungsi Python menjadi kode mesin yang dioptimalkan. Hal inilah yang menyebabkan waktu eksekusi kode Python menjadi lebih cepat.

5. Galois

Galois adalah *library* tambahan pada Python yang digunakan untuk memudahkan operasi pada lapangan hingga. *Library* ini dapat digunakan untuk mengkonstruksi lapangan galois dengan polinomial tak tereduksi tertentu. Generator dari lapangan galois juga dapat diketahui dari proses konstruksi ini.

## 3.5 Proses Validasi

Validasi dilakukan untuk menguji bahwa dekripsi dapat mengembalikan berkas gambar yang telah dienkripsi menjadi seperti semula. Pengujian dilakukan menggunakan program aplikasi yang dikonstruksi. Pengujian dilakukan terhadap gambar dengan jenis dan ukuran yang berbeda.

## 3.6 Penarikan Kesimpulan

Penarikan kesimpulan dilakukan terhadap penelitian yang telah dilakukan pada tahap akhir penelitian. Algoritma kriptografi valid jika dekripsi mengembalikan berkas gambar yang telah dienkripsi menjadi seperti semula.