BAB III
METODE PENELITIAN

Penelitian dilakukan dengan menggunakan metodologi studi literatur dan pengembangan model, serta pembuatan program aplikasi yang secara rinci diuraikan dalam langkah-langkah berikut:

3.1 Perumusan Masalah

Kriptografi terdiri dari dua proses yaitu enkripsi dan dekripsi. Untuk melakukan enkripsi dan dekripsi pesan, baik pengirim maupun penerima pesan harus memiliki buku kode yang sama. Buku kode dalam hal ini digunakan untuk mengimplementasikan suatu kode. Namun penyebaran buku kode tersebut dapat menimbulkan masalah karena kerahasiaan yang menjadi salah satu tujuan dalam kriptografi menjadi tidak aman. Oleh karena itu penggunaan kode digantikan dengan *cipher*. Salah satu algoritma kriptografi yang kurang aman adalah *Hill cipher* karena dapat dipecahkan dengan kriptanalisis *known plaintext attack* menggunakan perkalian matriks dan persamaan linier.

3.2 Model Dasar

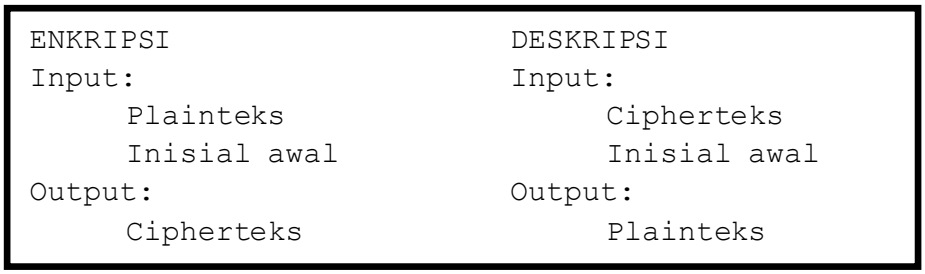
Model dasar yang digunakan adalah algoritma *Hill cipher, Convert Between Base* dan *Linear Feedback Shift Register*. Algoritma *Hill cipher* menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. *Convert Between Base* digunakan untuk mengkonversikan suatu basis ke basis lainnya, sedangkan *Linear Feedback Shift Register* digunakan untuk membangkitkan suatu kunci.

3.3 Pengembangan Model

Algoritma yang dirancang adalah modifikasi *Hill cipher* dengan menggunakan *Convert Between Base* dan *Linear Feedback Shift Register*. Algoritma tersebut kemudian dianalisa mengenai ketersediaan kunci dan kriptanalisis. Agar mempermudah proses enkripsi dan dekripsi, dilakukan pembuatan program.

3.4 Perancangan Program Aplikasi

Pada tahap ini dilakukan perancangan tampilan untuk program enkripsi dan dekripsi seperti pada Gambar 3.1. Input dari program enkripsi adalah inisial awal LFSR sebagai kunci dengan output cipherteks. Untuk proses dekripsi hampir sama, hanya saja plainteksnya sebagai output dan cipherteks sebagai input.



Gambar 3.1 Rancangan Program Enkripsi dan Dekripsi

3.5 Pembuatan Program Aplikasi

Program modifikasi *Hill cipher* dengan menggunakan *Convert Between Base* dan *Linear Feedback Shift Register* akan dibuat dengan menggunakan MATLAB. Program tersebut bertujuan agar mempermudah proses enkripsi dan dekripsi serta analisa untuk tahap selanjutnya.

3.6 Validasi

Pada tahap ini dilakukan validasi dari hasil output program yang diperoleh. Modifikasi algoritma *Hill cipher* dapat digunakan dan dianalisa perbandingan *Hill cipher* dengan modifikasi *Hill cipher* khususnya mengenai kebutuhan waktu.

3.7 Penarikan Kesimpulan

Pada tahap ini diperoleh beberapa kesimpulan berkaitan dengan tujuan penelitian.