BAB III
METODE PENELITIAN

Penelitian ini dilakukan dengan menggunakan studi literatur, pengembangan model kriptosistem gabungan dan implementasi model ke dalam program komputer, dengan rincian:

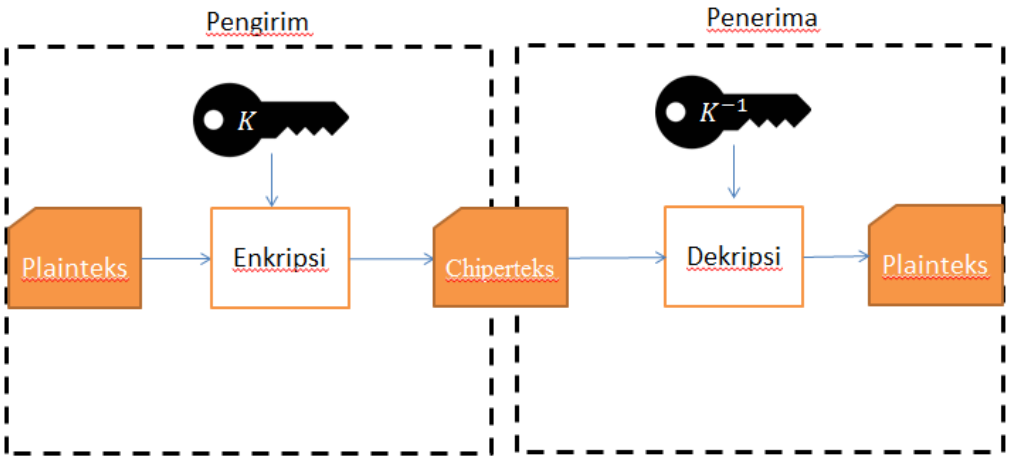
3.1 Identifikasi Masalah

Seiring dengan perkembangan kriptografi, sudah banyak kriptografi yang dapat dipecahkan. Contohnya kriptografi simetris hill cipher dan vignere cipher. Kedua kriptografi tersebut mempunyai kelemahan yang hampir mirip sehingga penggunaanya tidak banyak digunakan dalam pengamanan data atau pesan rahasia.

Maka untuk memperkuat kriptografi yang ada, dapat dilakukan dengan memodifikasi kriptografi. Kriptografi Hill cipher yang akan dimodifikasi dengan matriks sirkulan akan meningkatkan keamanan pesan atau data rahasia ditambah dengan vigenere yang menggunakan bilangan ASCII dalam proses kriptografi.

3.2 Model Dasar

Hill cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kirptografi ini menggunakan sebuah matriks persegi $m \; x \; m$ sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi



Gambar 3.1 Skema *Hill Cipher*

Pada skema algoritma *Hill Cpher* diatas, kunci pada melakukan enkripsi dan dekripsi merupakan kunci simetris. Sehingga pada model yang dikembangkan ini menggunakan matriks sirkulan untuk membuat sebuah kunci baru pada algoritma *Hill cipher*.

3.3. Pengembangan Kriptografi *Hill cipher* dengan matriks sirkulan

Pada penelitian ini akan dirancang sebuah kriptosistem Hill cipher yang baru. Tujuannya adalah untuk membentuk sebuah kriptosistem baru yang lebih aman. Langkah pertama adalah memilih matriks privat dan matriks publik untuk proses pembangkitan kunci, kemudian membangkitkan kunci enkripsi dan dekripsi. Selanjutnya plainteks di enkripsi dengan kunci yang sudah dibuat. Untuk mempermudah proses enkripsi dan dekripsi, dilakukan pembuatan program komputer.

3.4 Konstruksi Program Aplikasi

Program aplikasi ini dikonstruksi menggunakan *software* Matlab R2016a. Adapun tahapan dalam proses kontruksi program aplikasi antara lain :

1. Penentuan masukan dan keluaran
2. Rancangan tampilan program aplikasi
3. Algoritma program aplikasi
4. *Coding*

3.5 Validasi

Validasi dilakukan untuk mengetahui apakah kriptografi modifikasi *Hill Cipher* dengan matriks sirkulan dapat dienkripsi dan didekripsi dengan baik atau tidak.

3.6 Kesimpulan

Hasil dari penggabungan dua kriptografi ini adalah algoritma klasik vigenere yang diperkuat dengan algoritma *Hill Cipher* yang telah dimodifikasi dengan matriks sirkulan yang tidak mudah untuk dipecahkan. Sehingga pesan yang dikirimkan mempunyai tingkat kemanan yang lebih tinggi.