BAB III
METODE PENELITIAN

Penulisan skripsi ini merupakan suatu studi literatur dan pengembangan model, serta pembuatan program aplikasi yang secara rinci diuraikan dalam langkah-langkah berikut:

3.1 Perumusan Masalah

Hill Cipher merupakan teknik kriptografi klasik yang memanfaatkan matriks dalam mensubstitusi huruf-huruf dalam pesan yang akan dienkripsi. Teknik ini sulit untuk dipecahkan dengan frekuensi huruf tunggal karena setiap huruf pada pesan akan saling mempengaruhi perubahan huruf lainnya. Namun teknik ini dapat dipecahkan dengan metode *known-plaintext* yaitu dengan mengetahui sedikit dari *plaintext* pesan dan panjang kunci matriksnya. Untuk mengantisipasi hal tersebut algoritma *Hill Cipher* akan dimodifikasi dengan menambah algoritma serta memperpanjang kunci matriksnya. Selain itu, untuk mempermudah perhitungan, akan dibuat program aplikasi untuk mempermudah penggunaan teknik tersebut.

3.2 Model Dasar

Sebelum membangun algoritma, terlebih dahulu harus mengetahui teori yang mendasari algoritma ini. Hal pertama yang menjadi modal dasar adalah algoritma *Hill Cipher*. *Hill Cipher* termasuk dalam salah satu kriptosistem polialfabetik, artinya setiap karakter alfabet bisa dipetakan ke lebih dari satu macam karakter alfabet. Cipher ini ditemukan pada tahun 1929 oleh Lester S. Hill. Misalkan m adalah bilangan bulat positif, P adalah *plaintext* dan C adalah *ciphertext* dan $P = C = (Z_{26})^m$. Ide dasar dari *Hill Cipher* adalah dengan mengambil kombinasi linear dari m karakter alfabet dalam satu elemen *plaintext*, sehingga menghasilkan m alfabet dalam satu elemen *plaintext*.

Misalkan m = 2, maka kita dapat menuliskan suatu elemen *plaintext* sebagai $x = (x_1 , x_2)$ dan suatu *ciphertext* sebagai $y = (y_1 , y_2)$. Dimana y_1 , y_2 adalah kombinasi linear dari x_1 dan x_2. Misalkan

$y_1 = 5\ x_1 + 2x2$

$y_2 = 4\ x_1 + 3\ x2$

Kombinasi linear di atas dapat dituliskan dalam bentuk persamaan matriks. Dengan K sebagai matriks kunci, maka diperoleh Y=KX sebagai algoritma enkripsi dari *Hill Cipher*. Kemudian apabila kedua ruas dikalikan dengan invers dari kunci dan dengan memanfaatkan sifat sifat matriks maka akan diperoleh

$K^{-1}Y=K^{-1}KX$

$K^{-1}Y=IX$

$X=K^{-1}Y$

3.3 Pengembangan Model

Hill Cipher dapat dipecahkan dengan teknik *known-plaintext*. Maksudnya, apabila kriptanalis mendapatkan informasi tentang panjang kunci dan sedikit potongan *plaintext* maka ia dapat mengetahui kunci apa yang digunakan. Maka dari itu, *Hill Cipher akan* dimodifikasi dengan cara berikut.

1. Menambah karakter (spasi) , (titik) , (koma) sehingga banyak karakter yang tersedia menjadi 29.
2. Menambah algoritma dengan memanfaatkan transpos dari kunci matriks yang dimiliki, serta memanfaatkan perbedaan dari Y = XK dengan Y = KX pada perkalian matriks.
3. Panjang algoritma disesuaikan dengan keinginan pengguna

Karena algoritma ini berbentuk seperti rantai, maka algoritma ini disebut dengan *Chain Hill Cipher*.

3.4 Perancangan Model Aplikasi

Algoritma yang sudah dibangun, selanjutnya dapat diterapkan ke dalam aplikasi MATLAB untuk mempermudah proses enkripsi dan dekripsi. Untuk membuat program aplikasi, diperlukan prosedur yang tepat agar algoritma yang dimiliki dapat dimengerti dan dijalankan oleh program aplikasi tersebut. Adapun *interface* yang diharapkan adalah tampilan sederhana dimana pengguna program aplikasi dapat dengan mudah menggunakan algoritma *Chain Hill Cipher* dalam mengenkripsi dan mendekripsi pesan. Selain itu, pengguna dapat menentukan sendiri kunci matriks dan panjang rantai yang akan digunakan.

3.5 Program Aplikasi

Dengan tampilan satu jendela, dimana terdapat kolom opsi algoritma (enkripsi atau dekripsi), kolom pesan enkripsi, kolom pesan dekripsi, kolom kunci matriks dan kolom panjang rantai, diharapkan dapat mempermudah pengguna dalam memanfaatkan program aplikasi tersebut.

3.6 Validasi

Pada tahap ini dilakukan validasi dari hasil output pogram yang diperoleh. Algoritma *Chain Hill Cipher* yang diaplikasikan ke dalam program akan disesuaikan dengan perhitungan manualnya.

3.7 Penarikan Kesimpulan

Pada tahap ini diperoleh beberapa kesimpulan berkaitan dengan tujuan penelitian