BAB V
KESIMPULAN DAN SARAN

5.1.Kesimpulan

Berdasarkan penelitian ini, dapat ditarik kesimpulan sebagai berikut:

1. Modifikasi kriptografi *Hill cipher* dengan matriks sirkulan adalah kriptografi yang menggunakan konsep matriks sirkulan untuk membuat sebuah kunci publik dan kunci privat di mana kedua kunci tersebut akan dikombinasikan menjadi kunci utama dalam enkripsi dan dekripsi suatu pesan atau cipherteks.
2. Pada proses pembangkitan kunci publik, matriks kunci publik, misalkan $\mathrm{G} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dengan $G_c = \begin{pmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{pmatrix}$ memiliki 4 solusi alternatif untuk membangkitkan matriks kunci publik antara lain :
    a. Solusi 1: $b = b,\ c = c,\ d = d,\ a = -b + c + d$
    b. Solusi 2 : $b = b,\ c = c,\ d = d,\ a = -b - c - d$
    c. Solusi 3 $b = b,\ c = c,\ d = d,\ a = b - c + d$
    d. Solusi 4. $b = b,\ c = c,\ d = d,\ a = b + c - d$
3. Implementasi modifikasi kriptografi *Hill cipher* dengan matriks sirkulan dilakukan menggunakan bahasa pemrograman MATLAB berupa program komputer. Implementasi dilakukan menggunakan GUIDE sebagai salah satu fitur dalam MATLAB untuk membuat *Unit Interface* program. Program komputer tersebut digunakan untuk mempermudah pengguna (baik pengirim maupun penerima pesan) untuk melakukan pembangkitan kunci, enkripsi dan dekripsi.

5.2 Saran

Adapun saran dari penulis untuk penelitian ini adalah:

1. Peneliti selanjutnya diharapkan dapat menganalisa keamanan modifikasi kriptografi *Hill cipher* dengan matriks sirkulan secara lebih mendalam.
2. Dalam penelitian selanjutnya, dapat dikaji apakah representasi plaintext dapat menggunakan sistem Unicode untuk mendukung huruf-huruf selain huruf Latin dan emoji.
3. Dapat pula dikaji apabila dapat menggunakan matriks $3x3$ hinga matriks $n\ x\ n$ agar matriks yang digunakan lebih beragam.