PENGIMPLEMENTASIAN MODIFIKASI KRIPTOGRAFI *HILLCIPHER* DENGAN MATRIKS SIRKULAN

Muhammad Hilman Adiwibawa*, Rini Marwati, Ririn Sispiyati
Departemen Pendidikan Matematika FPMIPA UPI
*Surel :hilman.adiwibawa@gmail.com

ABSTRAK Dengan semakin maju teknologi informasi, maka semakin besar pula celah keamanan saat berkomunikasi. Masalah yang dikaji pada penelitian ini yaitu pengimplementasian modifikasi kriptografi *Hillcipher* dengan matriks sirkulan. Metode kriptografi ini menggunakan matriks sirkulan dalam pembangkitan matriks kunci publik dan pemilihan kunci privat, sehingga kunci yang semula simetris berubah menjadi kunci asimetris. Selanjutnya dibuat program aplikasi kriptografi tersebut yang bertujuan untuk memudahkan pengguna memakai algoritma modifikasi kriptografi. Dalam program aplikasinya menggunakan 95 karakter dari bilangan ASCII sehingga lebih banyak karakter dalam enkripi dan dekripsi.

Kata Kunci: Kriptografi, *Hill Cipher*, Matriks Sirkulan

ABSTRACT Development technology information has increasing from year to year. With development of technology, security gap in communication is become wider.To overcome this issues,we need cryptography knowledge. The problem that will be examined in this study is it implementation of modified cryptography *Hillcipher* with circulant matrices. This cryptography method using circulant matrices in generating public key matrices and choosing private key. So that, a key that we used from simetric key becomes asimetric key. Furthermore, cryptography application will be made which it aims to facilitate users in using the modified cryptography. In this prorgram, we used 95 characters in ASCII numbers so we can use more character in encryption and decryption.

Kata Kunci: Cryptography, *Hill Cipher*, circulant matrices.

1. PENDAHULUAN

Di era teknologi zaman sekarang, informasi merupakan hal yang penting dan vital untuk setiap orang. Apabila suatu informasi berupa percakapan bocor ke orang yang tidak berhak, hal tersebut dapat memberikan kerugian yang sangat besar kepada kedua belah pihak terkait. Terlebih lagi, dengan perkembangan pesat teknologi internet, celah untuk mencuri informasi data perusahaan lebih besar. Untuk mengatasi masalah keamanan tersebut, dibutuhkan ilmu kriptografi yang berguna untuk menyembunyikan informasi secara rahasia.

Hillcipher merupakan penerapan aritmatika modulo pada kriptografi.Teknik kriptografi ini menggunakan sebuah matriks persegi berukuran mxm sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Kekurangan pada kriptografi *Hillcipher* adalah matriks kunci yang digunakan untuk enkripsi dan deskripsi adalah sama, dan karakter yang dapat digunakan bersifat terbatas, yaitu hanya karakter alphabet. Menggunakan metode *known plaintext attack*, kriptografi *Hill cipher* sudah bisa ditembus sehingga tingkat keamanan metode kriptografi ini sudah tidak aman. Salah satu cara untuk memperkuat keamanan dari kriptografi *Hill cipher* adalah dengan menggunakan matriks sirkulan.

Penggunaan matriks sirkulan terdapat di AES (*Advanced Encryption System*) pada tahap Mix Coloumns. Selain itu, matriks sirkulan juga terdapat pada kriptografi WHIRLPOOL yaitu pada tahap Shift Coloumns. Kelebihan dari matriks sirkulan pada kriptografi adalah mengurangi kunci yang semula berjumlah $n^2 \in Z_p$ menjadi n buah elemen sehingga dapat mempercepat waktu proses penghitungan pada program aplikasi dan dapat mengurangi memori yang digunakan.

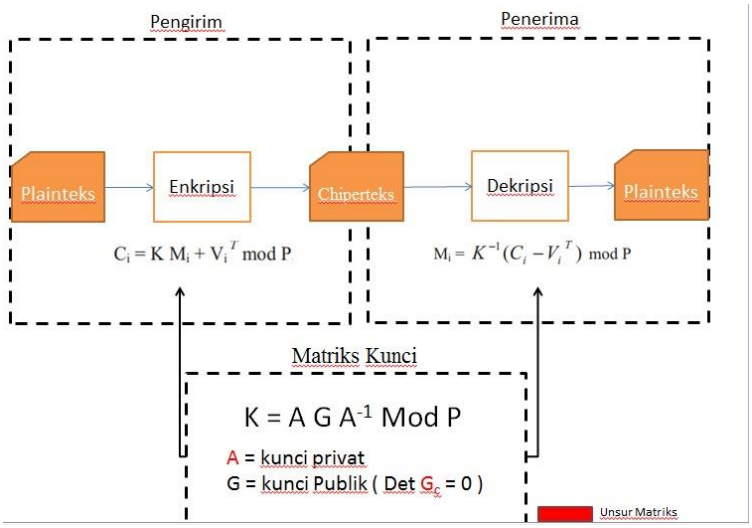
Oleh karena itu, dalam penelitian ini penulis memodifikasi kriptografi *Hillcipher* dengan melibatkan matriks sirkulan. Pada artikel ini akan dipaparkan konsep dan algoritma kriptografi *Hillcipher* yang dimodifikasi dengan matriks sirkulan, cara pembangkitan kunci publiknya, dan hasil pengimplementasian algoritma kriptografi tersebut pada bahasa pemrograman MatLab.

2. METODOLOGI

Pada penelitian ini dirancang sebuah kriptosistem Hill cipher yang baru agar tingkat keamanan lebih tinggi. 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 aplikasi menggunakan MatLab dengan tahapan-tahapan: penentuan masukan dan keluaran, rancangan tampilan program aplikasi, algoritma program aplikasi, dan coding. Validasi pada program aplikasi dengan cara mencocokan masukan dan keluaran program aplikasi dengan perhitungan matematika secara manual, apabila terdapat kesamaan maka validasi dianggap berhasil.

3. HASIL/TEMUAN DAN PEMBAHASAN

Berikut skema algoritma modifikasi kriptografi *Hill cipher* dengan matriks sirkulan



Gambar 1. Skema alur modifikasi kriptografi *Hill cipher* dengan matriks sirkulan

Skema pada Gambar 1 dapat diwujudkan dalam langkah-langkah algoritma kriptografi sebagai berikut:1. Pembangkitan kunci Publik (G); 2. Proses enkripsi; 3. Proses dekripsi.

Dalam proses pembangkitan matriks kunci publik *Hillcipher*, langkah-langkah yang digunakan adalah sebagai berikut:

1. Diketahui sebuah matriks ditulis sebagai berikut :
$$G = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
2. Konstruksi matriks G menjadi Koefisien matriks G_c ditulis sebagai berikut:
$$G_c = \begin{pmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{pmatrix}$$
3. Hitung determinan G_c sedemikian sehingga det(G_c) = 0
$$a^4 - 2a^2b^2 + 8adbc - 2d^2a^2 - 2c^2a^2 + b^4 - 2d^2b^2 - 2c^2b^2 + c^4 - 2c^2d^2 + d^4 = 0$$
4. Diperoleh empat solusi yang mungkin untuk persamaan di atas, yaitu:
Solusi 1: $b = b, c = c, d = d, a = -b + c + d$
Solusi 2: $b = b, c = c, d = d, a = -b - c - d$
Solusi 3: $b = b, c = c, d = d, a = b - c + d$
Solusi 4: $b = b, c = c, d = d, a = b + c - d$

5. Pilih salah satu dari empat solusi tersebut, kemudian ambil b, c, d secara acak
Contoh:
$$b = 11, c = 21, d = 3, a = -11 + 21 + 3 = 13$$
6. Maka matriks G adalah sebagai berikut
$$G = \begin{pmatrix} 13 & 11 \\ 21 & 3 \end{pmatrix}$$

Proses enkripsi kriptografi *Hill cipher* dengan menggunakan matriks sirkulan menggunakan dua kunci, yaitu matriks sirkulan sebagai kunci privat dan matriks non singular sebagai kunci publik. Dalam pemilihan kunci publik dan kunci privat ada beberapa syarat yang harus dipenuhi, yaitu:

1. Kunci publik (G) adalah matriks non singular berukuran 2x2 di mana det (G) = 0
2. Kunci privat (A) adalah matriks sirkulan prima dimana $gcd(d, e) = 1$, $d, e \in Z$

Proses enkripsi kriptografi *Hill cipher* dengan menggunakan matriks sirkulan dapat dilakukan setelah memperoleh kunci publik dan kunci privat. Langkah-langkahnya adalah sebagai berikut:

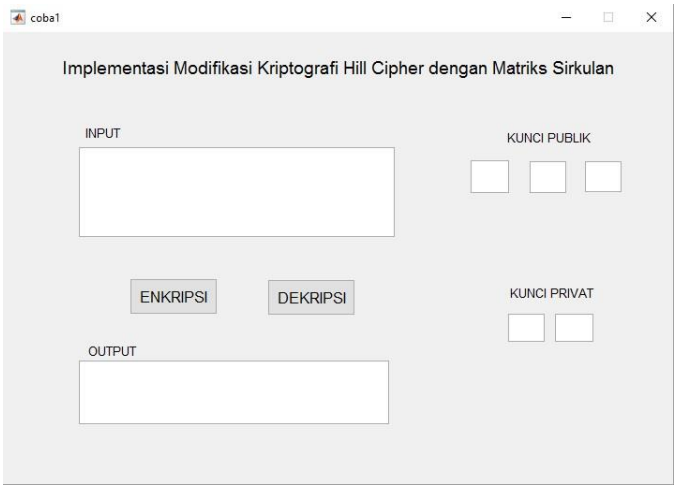
1. Diketahui plainteks $P \in \mathcal{P}$, matriks kunci privat A, dan matriks kunci public G
2. Konversi P ke bilangan desimal dalam kode ASCII.
3. Jika panjang plainteks $M = n$ sedemikian sehingga $mod(n, 2) \neq 0$, tambahkan *variable dummy* . Kemudian plainteks diubah menjadi blok plainteks (M)dengan ukuran baris 2
4. Hitung kunci utama yaitu K dengan rumus
$$K = AGA^{-1} \, mod \, 95$$
5. Selanjutnya, proses enkripsi menggunakan rumus di bawah ini :
$$C_i = K_i M_i + V_i^T mod \, 95.$$
Dengan V_i adalah baris ke-i dari matriks A
6. Konversi C dari bilangan desimal menjadi karakter berdasarkan kode ASCII, di sini yang digunakan adalah tabel ASCII 8 bit.
7. C merupakan cipherteks yang akan dikirim.

Proses dekripsi kriptografi *Hill* cipher dengan menggunakan matriks sirkulan menggunakan dua kunci seperti pada proses enkripsi, yaitu matriks sirkulan sebagai kunci privat dan matriks non singular sebagai kunci publik. Berikut proses dekripsi:

1. Diketahui cipherteks C, kunci privat A, dan kunci publik G
2. Konversi C ke bilangan desimal dalam kode ASCII. Kemudian cipherteksdiubah menjadi blok cipherteks dengan ukuran baris 2
3. Bangkitkan kunci utama yaitu K^{-1} dengan rumus
$$K^{-1} = AG^{-1}A^{-1} \, mod \, 95 \qquad (4.2)$$
4. Selanjutnya, proses dekripsi menggunakan rumus di bawah ini :
$$M_i = K^{-1}(C_i - V_i^T) \, mod \, 95.$$
5. Di mana V_i adalah baris ke-i dari matriks A

6. Konversi M dari bilangan decimal menjadi karakter berdasarkan kode ASCII, di sini yang digunakan adalah tabel ASCII 8 bit.
7. Ubah blok plainteks M menjadi plainteks P
8. P merupakan plainteks yang diterima

Program aplikasi kriptografi diimplementasikan sesuai dengan perancangan program aplikasi yang telah dibuat menggunakan bahasa pemograman Matlab R2016a



Gambar 2. Tampilan *user view*

Cara pemakaian program ini sangat mudah, untuk proses enkripsi, user memasukan plainteks yang akan dibuat menjadi pesan rahasia pada kolom INPUT, kemudian user mengisi kotak pada kunci publik dan kunci privat untuk menginput matriks-matriks yang akan digunakan dalam enkripsi. Setelah semua terisi, tekan tombol ENKRIPSI untuk memulai proses enkripsi Sama halnya dengan cara pemakaian dekripsi, cipherteks yang telah didapat dari pengirim, diisi pada kolom INPUT, kunci privat dan kunci publik juga diisi dengan nilai yang sama saat proses enkripsi.

Berikut, validasi program aplikasi untuk proses enkripsi dan dekripsi

Proses Enkripsi

1. Masukan kata "$aku\ hilman$" pada input program
2. Masukan nilai $b = 3, c = 7, d = 1$, tekan tombol *generate*, maka akan tersimpan matriks G

$$G = \begin{pmatrix} 5 & 3 \\ 7 & 1 \end{pmatrix}$$

3. Masukan nilai 37 dan 91 pada bagian kunci privat, tekan tombol *generate*, maka otomatis akan tesimpat matriks A dalam program

$$A = \begin{pmatrix} 37 & 91 \\ 91 & 37 \end{pmatrix}$$

4. Konversikan plainteks ke dalam bilangan decimal ASCII kemudian setiap elemen pada plainteks dikurangkan dengan angka 32

   65 75 85 0 72 73 76 77 65 78

5. Karena ukuran plainteks yaitu 1×10 maka tidak perlu ditambahkan *variable dummy*
6. Ubah ukuran plainteks menjadi matriks ukuran 2×5

$$M = \begin{pmatrix} 65 & 85 & 72 & 76 & 65 \\ 75 & 0 & 73 & 77 & 78 \end{pmatrix}$$

7. Kemudian hitung nilai K sebagai kunci matriks utama :

$$K = \begin{pmatrix} 37 & 91 \\ 91 & 37 \end{pmatrix}\begin{pmatrix} 5 & 3 \\ 7 & 1 \end{pmatrix}\begin{pmatrix} 37 & 91 \\ 91 & 37 \end{pmatrix} mod\ 95$$

$$K = \begin{pmatrix} 44 & 59 \\ 46 & 57 \end{pmatrix} mod\ 95$$

8. Hitung nilai C

$$C = \begin{pmatrix} 44 & 59 \\ 46 & 57 \end{pmatrix}\begin{pmatrix} 65 & 85 & 72 & 76 & 65 \\ 75 & 0 & 73 & 77 & 78 \end{pmatrix} + \begin{pmatrix} 37 & 91 & 37 & 91 & 37 \\ 91 & 37 & 91 & 37 & 91 \end{pmatrix} mod\ 95$$

$$C = \begin{pmatrix} 7 & 31 & 7 & 93 & 89 \\ 41 & 51 & 59 & 37 & 22 \end{pmatrix} mod\ 95$$

9. Tambahkan semua elemen pada C dengan bilangan 32

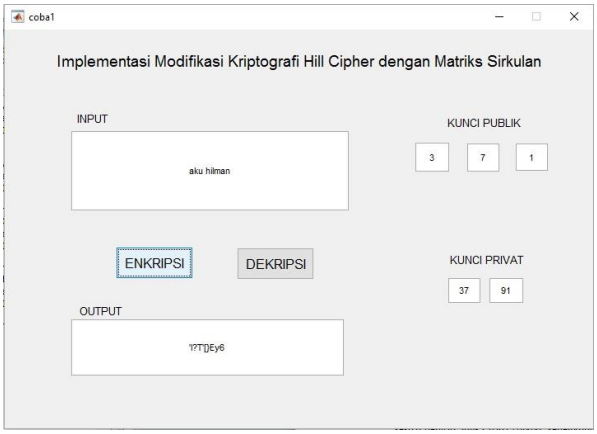
$$C = \begin{pmatrix} 39 & 63 & 39 & 125 & 121 \\ 73 & 84 & 91 & 69 & 54 \end{pmatrix}$$

10. Ubah bentuk Matriks menjadi $1\ x\ 10$

    39 73 63 84 39 91 125 69 121 54

11. Konversikan ke karakter ASCII

$$'I?\,T'[\}Ey6$$



Gambar 4. Contoh enkripsi

Proses Dekripsi

1. Masukan kata "$!?T'[}Ey6$" pada input program
2. Masukan nilai $b = 3, c = 7, d = 1$,, maka akan tersimpan matriks G
$$G = \begin{pmatrix} 5 & 3 \\ 7 & 1 \end{pmatrix}$$
3. Masukan nilai 37 dan 91 pada bagian kunci privat,maka otomatis akan tesimpan matriks A dalam program
$$A = \begin{pmatrix} 37 & 91 \\ 91 & 37 \end{pmatrix}$$
4. Konversikan *chipertext* ke dalam bilangan decimal ASCII kemudian setiap elemen pada plainteks dikurangkan dengan angka 32
7 41 31 52 7 59 93 37 89 22
5. Karena ukuran cipherteks yaitu 1×10 maka tidak perlu ditambahkan *variable dummy*
6. Ubah ukuran chiperteks menjadi matriks ukuran 2×5
$$C = \begin{pmatrix} 7 & 31 & 7 & 93 & 89 \\ 41 & 52 & 59 & 37 & 22 \end{pmatrix}$$
7. Kemudian hitung nilai K^{-1} sebagai kunci matriks utama :
$$K = \begin{pmatrix} 37 & 91 \\ 91 & 37 \end{pmatrix}\begin{pmatrix} 5 & 3 \\ 7 & 1 \end{pmatrix}\begin{pmatrix} 37 & 91 \\ 91 & 37 \end{pmatrix} mod\ 95$$
$$K = \begin{pmatrix} 38 & 86 \\ 69 & 21 \end{pmatrix} mod\ 95$$
8. Hitung nilai C

$$M = \begin{pmatrix} 38 & 86 \\ 69 & 21 \end{pmatrix}\left(\begin{pmatrix} 7 & 31 & 7 & 93 & 89 \\ 41 & 52 & 59 & 37 & 22 \end{pmatrix} - \begin{pmatrix} 37 & 91 & 37 & 91 & 37 \\ 91 & 37 & 91 & 37 & 91 \end{pmatrix}\right) mod\ 95$$

$$M = \begin{pmatrix} 65 & 85 & 72 & 76 & 65 \\ 75 & 0 & 73 & 77 & 78 \end{pmatrix} mod\ 95$$

9. Tambahkan semua elemen pada M dengan bilangan 32

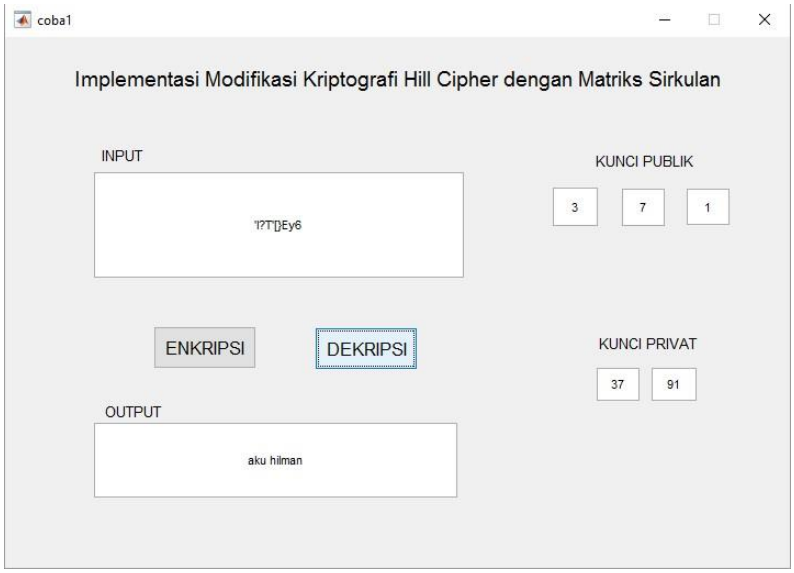
$$C = \begin{pmatrix} 97 & 117 & 104 & 108 & 97 \\ 107 & 32 & 105 & 109 & 110 \end{pmatrix}$$

10. Ubah bentuk Matriks menjadi $1\ x\ 10$

    97 107 117 32 104 105 108 109 97 110

11. Konversikan ke karakter ASCII

aku hilman



Gambar 5.Contoh Dekripsi

Berikut, analisa Keamanan Kriptografi *Hill cipher* dengan Matriks Sirkulan. Misalkan $A = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$, $A^{-1} = \begin{bmatrix} c & d \\ d & c \end{bmatrix}$, $G = \begin{bmatrix} G_1 & G_2 \\ G_3 & G_4 \end{bmatrix}$, dan $K = \begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix}$. Berdasarkan Algoritma Modifikasi Hill Cipher dengan matriks sirkulan didapat

$K = AGA^{-1} mod\ P$

$$\begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \begin{bmatrix} G_1 & G_2 \\ G_3 & G_4 \end{bmatrix} \begin{bmatrix} c & d \\ d & c \end{bmatrix}$$

$$\begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \begin{bmatrix} G_1c + G_2d & G_1d + G_2c \\ G_3c + G_4d & G_3d + G_4c \end{bmatrix}$$

$$\begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix}$$

$$= \begin{bmatrix} G_1ac + G_2ad + G_3bc + G_4bd & G_1ad + G_2ac + G_3bd + G_4bc \\ G_1bc + G_2bd + G_3ac + G_4ad & G_1bd + G_2bc + G_3ad + G_4ac \end{bmatrix}$$

$$\begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix}$$

$$= \begin{bmatrix} G_1ac + G_2ad + G_3bc + G_4bd & G_2ac + G_1ad + G_3bd + G_4bc \\ G_3ac + G_4ad + G_1bc + G_2bd & G_4ac + G_3ad + G_1bd + G_2bc \end{bmatrix}$$

$$\begin{bmatrix} K_1 \\ K_2 \\ K_3 \\ K_4 \end{bmatrix} = \begin{bmatrix} G_1 & G_2G_3 & G_4 \\ G_2 & G_1G_4 & G_3 \\ G_3 & G_4G_1 & G_2 \\ G_4 & G_3G_2 & G_1 \end{bmatrix} \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}$$

Karena $\det(G_c) = 0$, maka solusi yang didapat tak hingga karena jumlah persamaan kurang dari jumlah variabel yang tidak diketahui.

4. 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 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. DAFTAR PUSTAKA

[1] Anton, H., Rorres, C. (2004). *Aljabar Linear Elementer*. Jakarta: Erlangga

[2] Ariyus,D. 2008. *Pengantar Kriptografi : Teori, Analisis dan Implementasi*. Yogyakarta: ANDI.

[3] Cameron, P. J.(2003). *Notes on cryptography.* Diambil kembali dari http://ww.maths.qmw.ac.uk/~pjc/notes/crypt.pdf

[4] Burton, D.M. (2010). *Elementary Number Theory.* United States: McGraw-Hill.

[5] Davis, P.J. (1993). *Circulant Matrices.* United States :A Wiley-Interscience Publication.

[6] Menezes, A., Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography.* CRC Press. [7] Munir, R. (2006). *Kriptografi*. Bandung: Informatika.

[8] Munir, R. (2012). *Matematika Diskrit.* Bandung: Penerbit Informatika.

[9] Reddy, A. dkk. (2012). *A modified HIll Cipher Based on Circulant Matrices.* Procedia Technology. (4), .114-118.

[10] Stinson, D. (2006). *Cryptography: Theory and Practice, Third Edition.* Boca Raton, Florida: Chapman & Hall/CRC.

[11] Wikipedia. (2017). *ASCII*. Diambil kembali dari Wikipedia: https://en.wikipedia.org/wiki/ASCII, diakses pada tanggal 29 Desember 2017

[12] http://practicalcryptography.com/cryptanalysis/stochastic-searching/ cryptanalysis-hill-cipher/diakses pada tanggal 17 Januari 2018