Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI) **e-ISSN 2830-3954**
Volume: 1, Nomor : 2, September 2022 : 70-83 **p-ISSN 2830-6031**
https://jurnal.unity-academy.sch.id/index.php/jirsi/index

Menerapkan Algoritma *Hill Cipher* dan Matriks 2x2 Dalam Mengamankan *File* Teks Menggunakan Kode ASCII

Apply Hill Cipher Algorithm and 2x2 Matrix in Securing Text Files Using ASCII Code

Nurharianna Siregar*[1], Ilham Faisal[2], Divi Handoko[3]
[1,2,3]Teknik Informatika, Universitas Harapan Medan
E-mail: [1]hariannasiregar21@gmail.com, [2]ilhamoppa11@gmail.com, [3]divihandoko@gmail.com

Abstrak

Pada perkembangan teknologi saat ini, informasi (pesan) merupakan suatu kebutuhan pokok bagi masyarakat. Maka dari itu keamanan dari sebuah informasi sangatlah penting. Untuk mengamankan informasi tersebut dibutuhkan suatu teknik yang dapat mengamankan data, yaitu kriptografi. Oleh karena itu, penulis membuat suatu aplikasi yang dapat menjaga informasi yang bersifat rahasia. Pada aplikasi ini, penulis menggunakan sebuah metode kriptografi yaitu metode hill chiper, dimana hill chiper ini memiliki dua proses dalam menyandikan pesan yaitu enkripsi dan deskripsi. Dalam proses enkripsi dan deskripsi ini digunakan sebuah kunci matriks. Kunci matriks yang digunakan penulis adalah matriks 2x2. Pembuatan aplikasi ini menggunakan bahasa pemrograman phyton. Hasil yang akan dicapai dari penelitian ini adalah terciptanya sebuah aplikasi yang dapat menyandikan informasi (pesan) yang bersifat rahasia.

Kata kunci : *kriptografi, pesan, hill chiper, enkripsi, deskripsi*

Abstract

In today's technological developments, information (messages) is a basic need for society. Therefore the security of an information is very important. To secure the information required a technique that can secure the data, namely cryptography. Therefore, the author makes an application that can keep confidential information. In this application, the author uses a cryptographic method, namely the hill cipher method, where the hill cipher has two processes in encoding messages, namely encryption and description. In this encryption and description process, a matrix key is used. The matrix key used by the author is a 2x2 matrix. Making this application using the Python programming language. The result to be achieved from this research is the creation of an application that can encode confidential information (messages).

Keywords : *cryptography, message, hill cipher, encryption, description*

1. PENDAHULUAN

Pada zaman sekarang ini, sebuah *file* merupakan hal yang sangat penting bagi setiap orang, dimana banyak orang yang tidak memiliki hak ingin mengubah atau bahkan mengganti isi dari *file* yang disimpan, sehingga menyebabkan sering

terjadinya perubahan isi *file* yang telah disimpan. Dalam menyimpan *file,* terutama yang bersifat rahasia, *file* tersebut harus terlebih dahulu diamankan menggunakan algoritma *hill cipher.*

Hill Cipher merupakan salah satu algoritma kriptografi yang memanfaatkan matriks sebagai kunci untuk melakukan enkripsi dan Dekripsi dan aritmatika modulo[1]. Dengan metode *hill cipher* sebuah *file* akan susah untuk diganti atau dipahami isinya, dikarenakan adanya kunci rahasia yang digunakan untuk mengetahui makna dari sebuah *file* teks tersebut.

Menurut penelitian yang dilakukan oleh Wanto tahun 2016 mengenai Analisis Mengatasi *Sniffing* Dan *Spoofing* Menggunakan Metode Enkripsi Dan Dekripsi Algoritma *Hill Cipher*, Wanto menggunakan algoritma kriptografi *hill cipher* sebagai metode keamanan untuk enkripsi dan dekripsi suatu pesan yang disimpan dan dikirim sehingga dapat mengatasi *sniffing* dan *spoofing*[2].

Menurut Jurnal Bayu Firmanto tahun 2021 mengenai Perbandingan Hasil Optimasi Transposisi *Hill Cipher* dan *Vigenere Cipher* pada Citra Digital, menyimpulkan bahwa secara visual citra hasil enkripsi dengan algoritma *Hill Cipher* dengan optimasi transposisi menghasilkan citra yang acak dan tidak terbaca pola aslinya. Sedangkan citra hasil enkripsi dengan algoritma *Vigenere Cipher* dengan optimasi transposisi menghasilkan citra yang masih menunjukkan karakteristik citra aslinya hanya saja komposisi warnanya yang berubah. Bila jumlah karakter yang akan dikodekan bukan genap, maka huruf terakhir tidak punya pasangan, untuk kasus ini tambahkan saja huruf yang sama dengan yang terakhir tersebut sebagai pasangannya[3].

2. METODE PENELITIAN

Metode penelitian yang digunakan adalah kriptografi menggunakan algoritma algoritma *hill cipher.* Kriptografi *(Cryptography)* berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia. Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan rahasia[4]. Menurut Menezes kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, integritas data, serta autentikasi data. *Hill Cipher* adalah suatu algoritma simetris yang sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsinya.

2.1 Analisa Masalah

Perkembangan teknologi pada era sekarang ini menjaga keamanan data merupakan hal yang sangat penting. Pengiriman informasi tanpa adanya proses dalam penyembunyian pesan sangat tidak akan aman apalagi untuk pengiriman pesan yang bersifat rahasia. Masalah yang akan diselesaikan dengan menggunakan sistem ini adalah bagaimana mengamankan sebuah *file* teks baik secara manual maupun dengan format .txt dari pihak pihak luar yang tidak berhak untuk mengetahui informasi tersebut. Adapun masalah utama di dalam penelitian ini

adalah bagaimana cara menerapkan metode *hill cipher* dan kunci matriks 2x2 dalam proses penyandian *file* teks.
Oleh karena itu, dibuat sebuah aplikasi yang dapat menyembunyikan suatu data atau *file* teks yang tidak dapat diketahui oleh orang yang tidak berkepentingan. Pada penelitian kali ini akan dirancang sebuah aplikasi untuk penyandian pesan. Di dalam proses penyandian *file* teks metode *hill cipher* ini terdapat dua proses yaitu proses enkripsi dan dekripsi.

2.2 Teknik Enkripsi *Hill Cipher*

Enkripsi *(encryption)* adalah seni dari meng-encipher suatu data, yang menterjemahkan data tersebut menjadi suatu data yang tidak dapat sibaca oleh siapapun, tapi hanya dapat dibaca oleh penerima data yang dimaksud.
Berikut tahapan-tahapan algoritma enkripsi *Hill Cipher:*
a. Menentukan Plaintext, kemudian membagi plaintext per blok sesuai dengan jumlah blok matiks kunci
b. Menentukan matriks kunci yang akan digunakan (nilai determinasi matriks kunci harus nilai bilangan ganjil positif atau negatif).
c. Melakukan proses enkripsi menggunakan rumus : $\mathbf{C = M_k * M_p}$
Keterangan :
C = *Ciphertext*
M_k = Matriks Kunci
M_p = Matriks *Plaintext*

2.3 Teknik Dekripsi *Hill Cipher*

Dekripsi adalah proses pembuatan kembali data dari pesan yang di enkripsi. Proses dekripsi pada *Hill Cipher* pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (*invers*) terlebih dahulu.
Berikut ini tahapan-tahapan algoritma dekripsi *Hill Cipher* :
1. Menentukan nilai determinan matriks kunci

$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ~~det K~~ $= \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ = ad-bc

2. Menentukan invers modulo = det * b mod n=1

Keterangan :
det = nilai determinan kunci matriks
b = bilangan positif atau negatif
mod = sisa bagi
untuk mencari nilai b digunakan rumus : n(k) + 1/det, dengan cara menentukan nilai K menggunakan bilangan positif 0,1,2,3…. dst dan negatif -1,-2,-3,…. dst sampai hasil perhitungan mendapatkan nilai bilangan positif atau negatif.
3. Menentukan invers matriks kunci (M_k)

$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \longrightarrow K^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

4. Tentukan kunci dekripsi *hill cipher*

Nilai invers modulo * invers matriks kunci

5. Gunakan rumus dekripsi *hill cipher*

P = M*k*$^{-1}$ * M*c*

Keterangan :

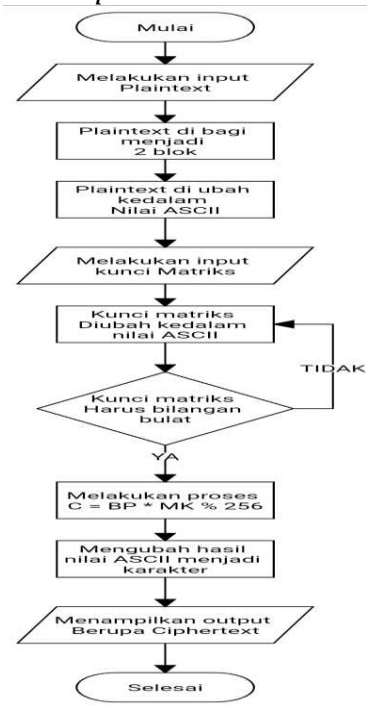
P = *Plaintext*

M*k* $^{-1}$ = Matriks kunci invers

2.4 *Flowchart*

Flowchart merupakan bagan *(Chart)* yang mengarahkan alir *(flow)* di dalam prosedur atau program sistem secara logika*[5]. Flowchart* adalah suatu diagram alir yang mempergunakan simbol atau tanda untuk menyelesaikan masalah. Untuk mengetahui bagaimana cara penyelesaian proses enkripsi dan dekripsi tersebut penulis telah membuat *flowchart* untuk proses enkripsi dan dekripsi dengan tujuan agar bisa mempermudah dalam pengerjaan enkripsi dan dekripsi. *Flowchart* enkripsi dan dekripsi bisa dilihat pada gambar 1 dan 2.

Untuk *flowchart* pada proses enkripsi bisa dilihat pada gambar 1 : Pada gambar 1 ini menjelaskan bagaimana proses enkripsi penyandian pesan dengan metode *hill cipher.* Pertama memasukkan *plaintext* (pesan) yang akan di enkripsi, setelah itu mengubah nilai *plaintext* (pesan) dalam bentuk ASCII, kemudian memasukkan kunci matriks yang akan digunakan dalam proses enkripsi, setelah itu menjumlahkan matriks kunci dengan matriks *plaintext* (pesan) yang sudah diubah dalam bentuk ASCII, kemudian mengubah nilai hasil dari penjumlahan matriks kunci dengan matriks *plaintext* (pesan) tersebut dalam bentuk huruf, setelah diubah maka akan menghasilkan *ciphertext*



Gambar 1 *Flowchart* Proses enkripsi *hill cipher*

Contoh :
Proses Enkripsi
a. Masukan *Plaintext*
Unhar Medan
b. Mengubah Nilai *Plaintext* ke Desimal
Un = $\begin{bmatrix} 85 \\ 110 \end{bmatrix}$ ha = $\begin{bmatrix} 104 \\ 97 \end{bmatrix}$ r spasi = $\begin{bmatrix} 114 \\ 32 \end{bmatrix}$
Me = $\begin{bmatrix} 77 \\ 101 \end{bmatrix}$ da = $\begin{bmatrix} 100 \\ 97 \end{bmatrix}$ nn = $\begin{bmatrix} 110 \\ 110 \end{bmatrix}$
c. Masukkan Kunci Matriks
$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix}$ ASCII $\begin{bmatrix} 52 & 51 \\ 51 & 51 \end{bmatrix}$
d. Jumlahkan Matriks K dengan Matriks P mod n (mod 26)

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix}\begin{bmatrix} 52 & 51 \\ 51 & 51 \end{bmatrix} = \text{x Un} = \begin{bmatrix} 85 \\ 110 \end{bmatrix} = \begin{bmatrix} (52\ x\ 85) + & (51\ x\ 110) \\ (51\ x\ 85) + & (51\ x\ 110) \end{bmatrix} \bmod 256$$

$$\begin{bmatrix} 4420 & + & 5610 \\ 4335 & + & 5610 \end{bmatrix} \bmod 256 = \begin{bmatrix} 10030 \\ 9945 \end{bmatrix} \bmod 256$$

$$= \begin{bmatrix} 46 \\ 217 \end{bmatrix} = .\grave{U}$$

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix}\begin{bmatrix} 52 & 51 \\ 51 & 51 \end{bmatrix} = \text{x ha} = \begin{bmatrix} 104 \\ 97 \end{bmatrix} = \begin{bmatrix} (52\ x\ 104) + & (51\ x\ 97) \\ (51\ x\ 104) + & (51\ x\ 97) \end{bmatrix} \bmod 256$$

$$\begin{bmatrix} 5408 & + & 4947 \\ 5304 & + & 4947 \end{bmatrix} \bmod 256 = \begin{bmatrix} 10355 \\ 10251 \end{bmatrix} \bmod 256$$

$$= \begin{bmatrix} 115 \\ 11 \end{bmatrix} = \text{s[]}$$

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix}\begin{bmatrix} 52 & 51 \\ 51 & 51 \end{bmatrix} = \text{x r spasi} = \begin{bmatrix} 114 \\ 32 \end{bmatrix} = \begin{bmatrix} (52\ x\ 114) + & (51\ x\ 32) \\ (51\ x\ 114) + & (51\ x\ 32) \end{bmatrix} \bmod 256$$

$$\begin{bmatrix} 5928 & + & 1632 \\ 5814 & + & 1632 \end{bmatrix} \bmod 256 = \begin{bmatrix} 7560 \\ 7446 \end{bmatrix} \bmod 256$$

$$= \begin{bmatrix} 136 \\ 22 \end{bmatrix} = \hat{}\ []$$

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix}\begin{bmatrix} 52 & 51 \\ 51 & 51 \end{bmatrix} = \text{x Me} = \begin{bmatrix} 77 \\ 101 \end{bmatrix} = \begin{bmatrix} (52\ x\ 77) + & (51\ x\ 101) \\ (51\ x\ 77) + & (51\ x\ 101) \end{bmatrix} \bmod 256$$

$$\begin{bmatrix} 4004 & + & 5151 \\ 3927 & + & 5151 \end{bmatrix} \bmod 256 = \begin{bmatrix} 9155 \\ 9078 \end{bmatrix} \bmod 256$$

$$= \begin{bmatrix} 195 \\ 118 \end{bmatrix} = \tilde{A}v$$

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix}\begin{bmatrix} 52 & 51 \\ 51 & 51 \end{bmatrix} = \text{x da} = \begin{bmatrix} 100 \\ 97 \end{bmatrix} = \begin{bmatrix} (52\ x\ 100) + & (51\ x\ 97) \\ (51\ x\ 100) + & (51\ x\ 97) \end{bmatrix} \bmod 256$$

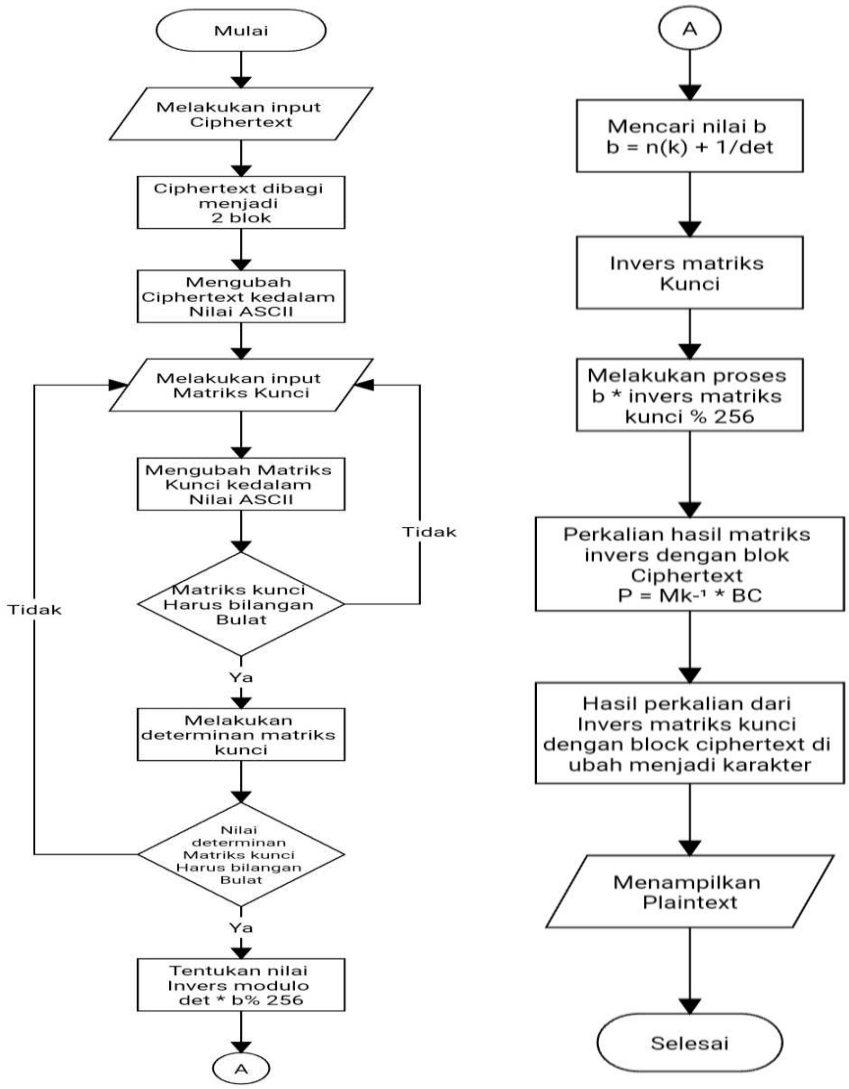
$$\begin{bmatrix} 5200 & + & 4947 \\ 5100 & + & 4947 \end{bmatrix} \bmod 256 = \begin{bmatrix} 10147 \\ 10047 \end{bmatrix} \bmod 256$$

$$= \begin{bmatrix} 163 \\ 63 \end{bmatrix} = \pounds?$$

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix}\begin{bmatrix} 52 & 51 \\ 51 & 51 \end{bmatrix} = \text{x nn} = \begin{bmatrix} 110 \\ 110 \end{bmatrix} = \begin{bmatrix} (52\ x\ 110) + & (51\ x\ 110) \\ (51\ x\ 110) + & (51\ x\ 110) \end{bmatrix} \bmod 256$$

$$\begin{bmatrix} 5720 & + & 5610 \\ 5610 & + & 5610 \end{bmatrix} \bmod 256 = \begin{bmatrix} 11330 \\ 11220 \end{bmatrix} \bmod 256 = \begin{bmatrix} 66 \\ 212 \end{bmatrix} = \text{BÔ}$$

Untuk *flowchart* pada proses dekripsi bisa dilihat pada gambar 2 : Pada gambar 2 diatas menjelaskan bagaimana proses dekripsi penyendian pesan dengan metode *hill cipher.* Pertama, masukkan cipherteks yang telah dihasilkan dari proses enkripsi sebelumnya, kemudian mengubah nilai cipherteks tersebut dalam bentuk desimal, kemudian masukkan kunci matriks yang akan digunakan, kemudian melakukan determinan kunci matriks yaitu dengan cara (K1*K4) – (K2*K3), kemudian setelah mendapatkan hasil determinan kunci selanjutanya yaitu melakukan invers modulo dengan cara : Det * b % 26 = 1, selanjutanya mencari nilai b, cara mencari nilai b yaitu: b = n(k) + 1 / det, dimana n merupakan jumlah seluruh abjad dan k merupakan sembarang angka yang apabila ditambah 1 lalu dibagi dengan hasil determinan menghasilkan bilangan bulat, sehingga bilangan bulat tersebut bisa digunakan sebagai nilai b. Selanjutnya yaitu invers matriks kunci yaitu : kunci a, b, c, d, menjadi kunci d, -b, -c, a, kemudian lakukan perkalian antara nilai b dengan invers matriks kunci lalu modulus 26 untuk mendapatkan kunci dekripsi yang akan digunakan, selanjutnya lakukan perkalian antara matriks kunci dekripsi dengan matriks cipherteks untuk mengembalikan cipherteks ke dalam bentuk plainteks.



Gambar 2 *Flowchart* Proses Dekripsi *hill cipher*

Contoh :

Proses Dekripsi

a. Masukan *Chipertext*

.Ù s[] ˆ [] Ãv £? BÔ

b. Mengubah Nilai *Chipertext* kedalam Desimal

$$\text{.Ù} = \begin{bmatrix}46\\217\end{bmatrix} \text{ s[] } = \begin{bmatrix}115\\11\end{bmatrix} \text{ ˆ [] } = \begin{bmatrix}136\\22\end{bmatrix}$$

$$\text{Ãv} = \begin{bmatrix}195\\118\end{bmatrix} \text{ £? } = \begin{bmatrix}163\\63\end{bmatrix} \text{ BÔ } = \begin{bmatrix}66\\212\end{bmatrix}$$

c. Masukan Kunci Matriks

$$\begin{bmatrix}4 & 3\\3 & 3\end{bmatrix} \text{ ASCII } \begin{bmatrix}52 & 51\\51 & 51\end{bmatrix}$$

d. Melakukan Determinan (K1 * K4) – (K2 * K3)

$\begin{bmatrix}52 & 51\\51 & 51\end{bmatrix}$= (52 x 51) – (51 x 51)

= 2.652 -2.601

= 51

e. Melakukan Invers Modulo

Det * b mod 256 = 1

51 * ( ) mod 256 = 1

f. Mencari Nilai b

b = n (k) + 1 / det

= 256 (50) + 1 / 51

= 12.800 + 1 / 51 = 12.801 / 51 = 251

g. Invers Matriks Kunci K

$\begin{bmatrix}52 & 51\\51 & 51\end{bmatrix}$= menjadi$\begin{bmatrix}51 & -51\\-51 & 52\end{bmatrix}$=

h. b * Invers Mk mod 256

$251\begin{bmatrix}51 & -51\\-51 & 52\end{bmatrix} = \begin{bmatrix}12.801 & -12.801\\-12.801 & 13.052\end{bmatrix} \bmod 256$

$= \begin{bmatrix}1 & 255\\255 & 252\end{bmatrix}$

i. $P = Mk^{-1} * MC$

$\begin{bmatrix}1 & 255\\255 & 252\end{bmatrix}$ x .Ù = $\begin{bmatrix}46\\217\end{bmatrix} = \begin{bmatrix}(1\ x\ 46) + & (255\ x\ 217)\\(255\ x\ 46) + & (252\ x\ 217)\end{bmatrix} \bmod 256 =$

$\begin{bmatrix}46 & + & 55.335\\11.730 & + & 54..684\end{bmatrix} \bmod 256 = \begin{bmatrix}55.381\\66.414\end{bmatrix} \bmod 256 = \begin{bmatrix}85\\110\end{bmatrix}$ = Un

$\begin{bmatrix}1 & 255\\255 & 252\end{bmatrix}$ x s[] = $\begin{bmatrix}115\\11\end{bmatrix} = \begin{bmatrix}(1\ x\ 115) + & (255\ x\ 11)\\(255\ x\ 115) + & (252\ x\ 11)\end{bmatrix} \bmod 256 =$

$\begin{bmatrix}115 & + & 2.805\\29.325 & + & 2.772\end{bmatrix} \bmod 256 = \begin{bmatrix}2.920\\32.092\end{bmatrix} \bmod 256 = \begin{bmatrix}104\\97\end{bmatrix}$ = ha

$\begin{bmatrix}1 & 255\\255 & 252\end{bmatrix}$ x ˆ [] = $\begin{bmatrix}136\\22\end{bmatrix} = \begin{bmatrix}(1\ x\ 136) + & (255\ x\ 22)\\(255\ x\ 136) + & (252\ x\ 22)\end{bmatrix} \bmod 256 =$

$\begin{bmatrix}136 & + & 5.610\\34.680 & + & 5.544\end{bmatrix} \bmod 256 = \begin{bmatrix}5.746\\40224\end{bmatrix} \bmod 256 = \begin{bmatrix}114\\32\end{bmatrix}$ = r spasi

$\begin{bmatrix}1 & 255\\255 & 252\end{bmatrix}$ x Ãv = $\begin{bmatrix}195\\118\end{bmatrix} = \begin{bmatrix}(1\ x195\ ) + & (255\ x\ 118)\\(255\ x\ 195) + & (252\ x\ 118)\end{bmatrix} \bmod 256 =$

$\begin{bmatrix}195 & + & 30.090\\49.725 & + & 29.736\end{bmatrix} \bmod 256 = \begin{bmatrix}30.285\\79.461\end{bmatrix} \bmod 256 = \begin{bmatrix}77\\101\end{bmatrix}$ = Me

$\begin{bmatrix}1 & 255\\255 & 252\end{bmatrix}$ x £? = $\begin{bmatrix}163\\63\end{bmatrix} = \begin{bmatrix}(1\ x\ 163\ ) + & (255\ x\ 63)\\(255\ x\ 163) + & (252\ x\ 63)\end{bmatrix} \bmod 256 =$

$\begin{bmatrix}163 & + & 16.065\\41.565 & + & 15.876\end{bmatrix} \bmod 256 = \begin{bmatrix}16.228\\57.441\end{bmatrix} \bmod 256 = \begin{bmatrix}100\\97\end{bmatrix}$ = da

$\begin{bmatrix}1 & 255\\255 & 252\end{bmatrix}$ x BÔ = $\begin{bmatrix}66\\212\end{bmatrix} = \begin{bmatrix}(1\ x\ 66\ ) + & (255\ x\ 212)\\(255\ x\ 66) + & (252\ x\ 212)\end{bmatrix} \bmod 256 =$

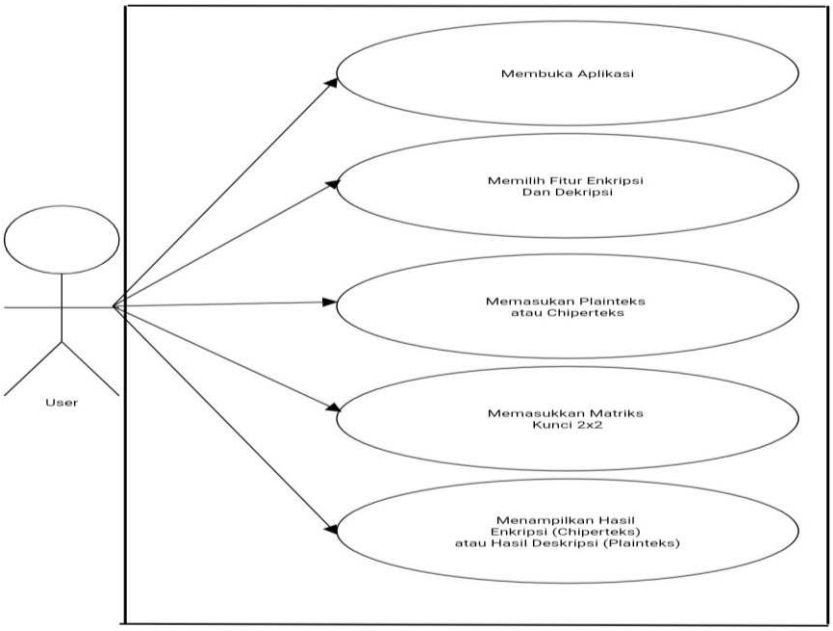
$\begin{bmatrix}66 & + & 54.060\\16.830 & + & 53.424\end{bmatrix} \bmod 256 = \begin{bmatrix}54.126\\70.254\end{bmatrix} \bmod 256 = \begin{bmatrix}110\\110\end{bmatrix}$ = nn

2.6 *UML (Unified Modeling Language)*

UML merupakan sebuah standar penulisan atau semacam *blue print* dimana didalamnya termasuk sebuah bisnis proses, penulisan kelas-kelas dalam sebuah bahasa yang spesifik[6]. Salah satu jenis dari uml (*unified modeling language*) adalah *use case.*

Use case diagram merupakan permodelan untuk kelakuan sistem informasi yang akan dibuat, *use case* diagram digunakan untuk mengetahui fungsi apa saja yang ada di dalam sistem dan yang berhak menggunakan fungsi – fungsi tersebut[7].

Use case diagram pada proses enkripsi dan dekripsi pada *hill cipher* bisa dilihat pada gambar 3



Gambar 3 *Use Case* Proses Enkripsi dan Dekripsi

Pada gambar 3 diatas, menjelaskan bagaimana *user* melakukan kegiatannya pada aplikasi penyandian pesan yang telah dibuat, berawal dari membuka aplikasi, kemudian memilih fitur apakah yang ingin dipilih baik enkripsi maupun dekripsi, kemudian memasukkan plainteks ataupun cipherteks yang akan disandikan, kemudian memasukkan kunci matriks 2x2 yang akan digunakan pada proses enkripsi dan dekripsi, selanjutnya setelah semuanya selesai maka akan tampil hasil berupa cipherteks jika yang dilakukan proses enkripsi, sebaliknya jika yang dilakukan proses dekripsi maka akan tampil plainteks.

3. HASIL DAN PEMBAHASAN

3.1 Tampilan Menu Utama Aplikasi

Pada saat aplikasi dijalankan, tampilan pertama yang akan muncul adalah tampilan menu utama yang didalamnya terdapat nama aplikasi, logo Universitas Harapan Medan, dan identitas peneliti serta tombol mulai yang berfungsi untuk memulai

penggunaan aplikasi. Tampilan menu utama pada aplikasi ini bisa dilihat pada gambar 4

Gambar 4 Tampilan Menu Utama Aplikasi

3.2 Tampilan Pilihan Fitur Aplikasi

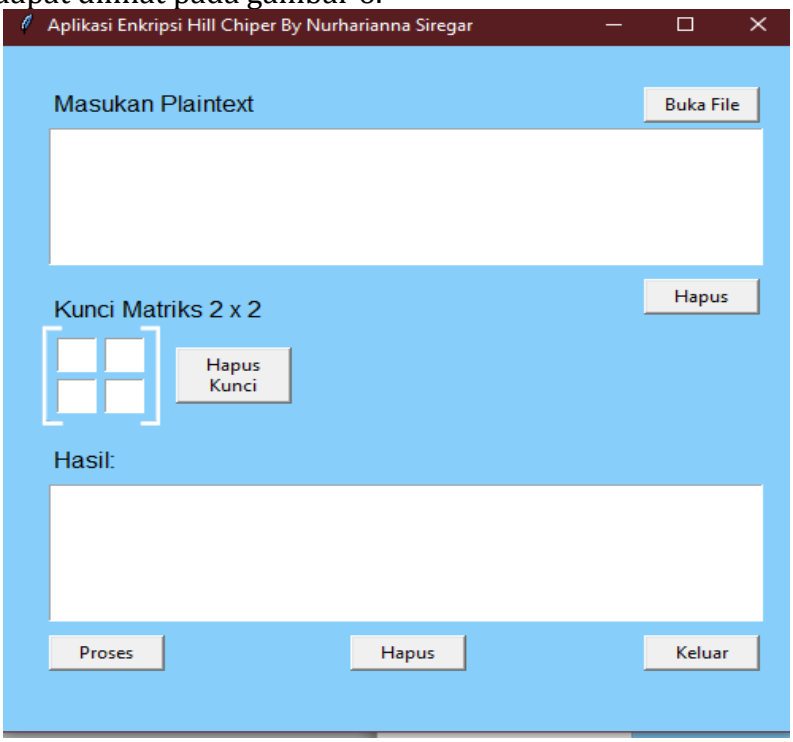
Saat *user* menekan tombol mulai yang terdapat pada menu utama maka tampilan akan berpindah ke tampilan selanjutnya yaitu tampilan pilihan fitur yang terdapat pada aplikasi. Dimana fitur yang terdapat pada aplikasi ini nantinya merupakan proses yang akan digunakan oleh *user* baik enkripsi, dekripsi maupun keluar dari aplikasi. Untuk tampilan pilihan fitur aplikasi bisa dilihat pada gambar 5.

Gambar 5 Tampilan Pilihan Fitur Aplikasi

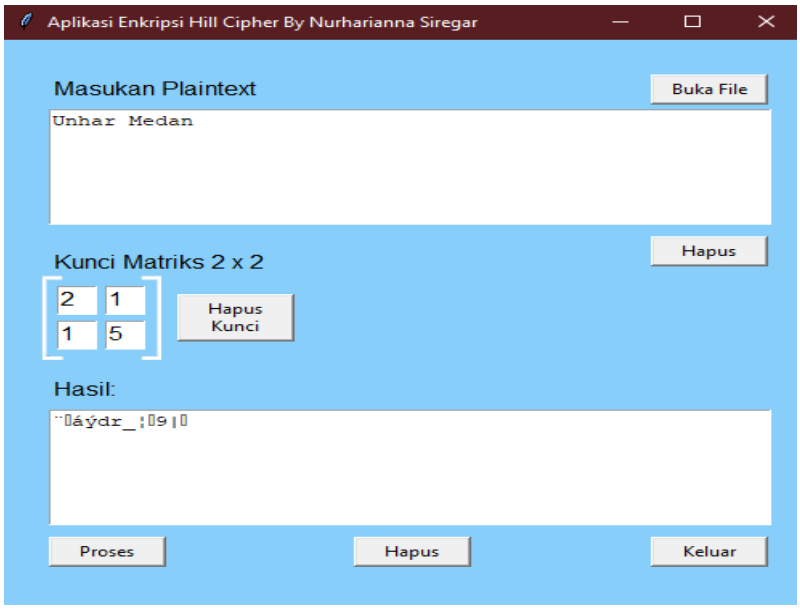
3.3 Tampilan Layar Proses Enkripsi

Saat *user* memilih proses enkripsi pada tampilan pilihan fitur maka selanjutnya *user* akan memulai proses pengerjaan enkripsi pada aplikasi. Pada tampilan proses enkripsi ini terdapat beberapa langkah untuk melakukan proses enkripsi yaitu pertama memasukkan *plaintext* (file dengan format *.txt) yang ingin di enkripsi,

kedua memasukkan kunci 1, kunci 2, kunci 3, dan kunci 4 yang ingin digunakan saat proses enkripsi, setelah semua kunci dimasukan maka akan tampil hasil berupa *ciphertext* dari pesan yang telah di enkripsi. Untuk tampilan proses enkripsi ini dapat dilihat pada gambar 6.



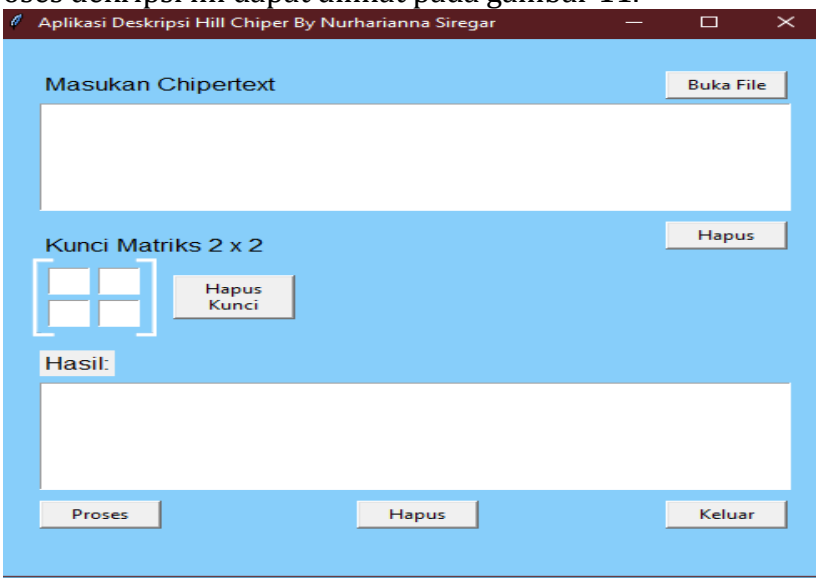
Gambar 6 Tampilan Layar Enkripsi



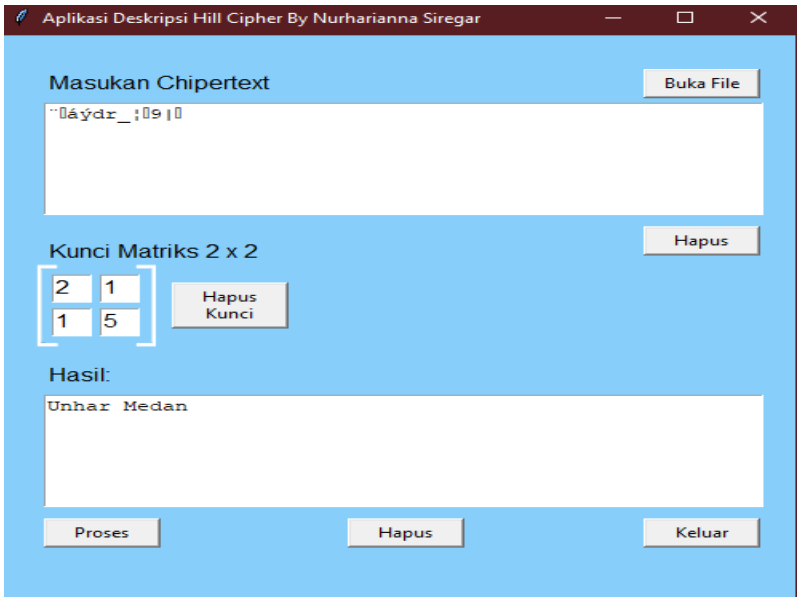
Gambar 7 Enkripsi Unhar Medan

3.5 Tampilan Layar Proses Dekripsi

Sebaliknya pada saat *user* memilih proses dekripsi pada tampilan pilihan fitur maka selanjutnya *user* akan memulai proses pengerjaan dekripsi pada aplikasi. Pada tampilan proses dekripsi ini terdapat beberapa langkah untuk melakukan proses dekripsi yaitu pertama memasukkan *ciphertext* (file dengan format *.txt) yang ingin di dekripsi, kedua memasukkan kunci 1, kunci 2, kunci 3, dan kunci 4 yang ingin digunakan saat proses dekripsi, setelah semua kunci dimasukan maka akan tampil hasil berupa *plaintext* dari pesan yang telah di dekripsi. Untuk tampilan proses dekripsi ini dapat dilihat pada gambar 11.



Gambar 11 Tampilan layar Dekripsi



Gambar 12 Dekripsi Unhar Medan

3.6 Pengujian Sistem *Black Box* Aplikasi

Hasil pengujian aplikasi *hill cipher* menggunakan pengujian sistem *black box* dapat dilihat pada tabel 1

Tabel 1 Pengujian *Black Box* Aplikasi

Aktivitas Pengujian	Realisasi Yang Diharapkan	Hasil Pengujian
Pilih fitur Enkripsi	Aplikasi bisa menampilkan form enkripsi	Form enkripsi berhasil di tampilkan
Pilih fitur Dekripsi	Aplikasi bisa menampilkan form dekripsi	Form dekripsi berhasil di tampilkan
Pilih fitur keluar aplikasi	Bisa keluar dari aplikasi	Berhasil keluar dari aplikasi

4. KESIMPULAN

4.1 Kesimpulan

Berdasarkan pengamatan yang dilakukan penulis sejak perancangan, pembuatan, hingga pengujian aplikasi maka diperoleh beberapa kesimpulan sebagai berikut :

1. Aplikasi *hill cipher* bisa memproses pesan sebanyak mungkin (pesan yang ingin di proses tidak dibatasi).
2. Aplikasi dapat memproses karakter,simbol dan angka
3. Kunci yang digunakan harus menghasilkan nilai bilangan bulat positif
4. Aplikasi memproses *file* menggunakan kunci matriks 2x2 dan hanya berupa angka
5. Aplikasi hanya dapat dijalankan di windows

4.2 Saran

Berikut ini adalah saran yang dapat digunakan untuk penelitian maupun pengembangan selanjutnya.

1. Untuk pengembangan sistem selanjutnya dapat menggunakan kombinasi algoritma kriptografi klasik dan kriptografi modern.

2. Sistem ini dapat menerima inputan file dengan format *.txt sehingga untuk penelitian selanjutnya diharapkan dapat menerima inputan file dengan format yang lain.
3. Sistem ini dapat bekerja pada pesan teks, sehingga untuk selanjutnya diharapkan bisa bekerja pada gambar dan video.
4. Sistem ini di implementasikan pada perangkat windows, sehingga untuk penelitian selanjutnya diharapkan dapat di implementasikan pada perangkat android maupun ios.
5. Bahasa pemrograman yang digunakan adalah *phyton.* Sehingga pada penelitian selanjutnya diharapkan dapat menggunakan bahasa pemrograman yang lain.

DAFTAR PUSTAKA

[1]. Hidayat, A., & Alawiyah, T. (2013). Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang. *Jurnal Matematika Integratif*, *9*(1), 39.

[2]. Dan, E., Algoritma, D., Chiper, H., Enkripsi, M., Dekripsi, D. A. N., & Hill, A. (2017). *ANALISIS MENGATASI SNIFFING DAN SPOOFING MENGGUNAKAN METODE*. (October 2015).

[3]. Firmanto, B., Putri, D., Ningrum, K., Bramanto, A., & Putra, W. (2021). Perbandingan Hasil Performa Optimasi Transposisi Hill Cipher dan Vigenere Cipher pada Citra Digital. *SMARTICS Journal*, *7*(2), 65–71. Retrieved from https://doi.org/10.21067/smartics.v7i2.5931

[4]. Yuliandaru, A. R. (2016). *Teknik Kriptografi Hill Cipher Menggunakan Matriks*.

[5]. Syamsiah, S.. (2019). *Perancangan flowchart dan pseudocode pembelajaran mengenal angka dengan animasi untuk anak paud rambutan*. *4*(1), 86–93.

[6]. Komputer, J. T., Harapan, P., & Tegal, B. (2018). *Unified Modeling Language (UML) Model Untuk Pengembangan Sistem Informasi Akademik Berbasis Web*. *03*(01), 126–129.

[7]. Supriadi, D., & Mugiati, R. (2018). *Sistem Informasi Pendaftaran Kursus Berbasis Web Pada Yayasan Musik Jakarta*. *3*(2).