APLIKASI MATRIK PADA ILMU KRIPTOGRAFI DENGAN MENGGUNAKAN MATLAB

Deby Erdriani[1)], Dewi Devita[2)]
[1]Fakultas Ilmu Komputer, Universitas Putra Indonesia "YPTK" Padang, Jln. Raya Lubuk Begalung Nan XX, Kec Lubuk Begalung, Kota Padang, Sumatera Barat
email: de2bye@upiyptk.ac.id

Abstrak

Penelitian kali ini mengenai hubungan matrik dengan kata sandi, untuk memberikan gambaran kepada mahasiswa khususnya mahasiswa jurusan komputer kalau matakuliah matrik bisa diaplikasikan pada kehidupan sehari hari, bahkan berhubungan dengan matakuliah kriptografi. Aplikasi matrik ini dicari menggunakan program Matlab dengan operasi matriks yaitu determinan dan invers. Kunci matriks berbentuk persegi dengan jumlah antara baris dan sama. Kunci matriks dengan ordo berapa pun akan lebih mudah mencarinya dengan menggunakan matlab. Makin besar ordo pada kunci matriks,maka makin aman kata sandi yang disampaikan kepada penerima pesan.

Keywords: Matriks, Determinan, Invers, Metode Hill Cipher dan Matlab

Abstract

This research is about the relationship between the matrix and passwords, to give an idea to students, especially students majoring in computers, that matrix courses can be applied in everyday life, even related to cryptography courses. This matrix application is searched using the Matlab program with matrix operations, namely determinant and inverse. The matrix key is a square with the sum between rows and equal. Matrix keys of any order will be easier to find using matlab. The larger the order in the key matrix, the more secure the password conveyed to the recipient of the message.

Keywords: *Matrix, Determinant, Inverse, Hill Cipher Method and Matlab*

1. PENDAHULUAN

Mahasiswa masih beranggapan kenapa mereka mempelajari ilmu lain yang tidak sesuai dengan jurusannya, kenapa tidak mempelajari mata kuliah sesuai dengan jurusan saja, jadi dalam pikiran mahasiswa itu masing beranggapan bahwa mereka tidak perlu atau bahkan mereka tidak butuh untuk mempelajari matakuliah yang tidak sesuai dengan jurusan yang diambil.

Matrik merupakan bagian ilmu matematika merupakan matakuliah dasar yang wajib diambil oleh mahasiswa. Sesuai dengan pengembangan kurikulum berdasarkan KKNI (Kerangka Kualifikasi Nasional Indonesia) Aptikom, Menerapkan matematika pengetahuan dasar ilmiah dan mekanisme kerja komputer sehingga mampu memecahkan masalah melalui pembuatan model solusi system berbasis komputer [5].

Pembahasan kali ini akan dibahas mengenai hubungan matrik dengan kata sandi, untuk memberikan gambaran kepada mahasiswa khususnya mahasiswa jurusan komputer kalau matakuliah matrik bisa diaplikasikan pada kehidupan sehari hari, bahkan berhubungan dengan matakuliah kriptografi.

Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan

Jurnal KomtekInfo, Vol.8 No.2Tahun 2021
e-ISSN: 2502-8758|| p-ISSN : 2356-0010
DOI: 10.35134/komtekinfo.v7i4
Page :154-162

suatu kunci enkrpsi menjadi suatu yang sulit dibaca oleh seseorang yang memiliki kunci deskripsi[6].

Tinjauan pustaka yang relevan yaitu M. Miftakul Amin pada penelitian yang berjudul implementasi kriptografi klasik pada komunikasi berbasis teks yang berpendapat bahwa kriptografi klasik sebagai metode untuk melakukan proses enkripsi dan deskripsi data teks yang dikirim melalui aplikasi chat. Dari proses pengujian diperoleh bahwa proses enskripsi dan deskripsi dapat menjadi kerahasian data[2].

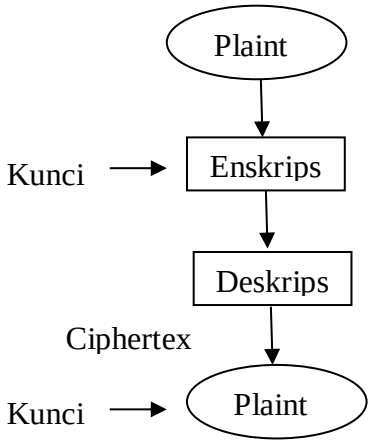
Menurut Sumadri penelitiannya yang berjudul Studi Model Algoritma Kriptografi Klasik dan Modern menyatakan bahwa tingkat keamanan, keefektifan dan koefisien kriptografi modern lebih terjamin dibandingkan kriptografi klasik[7].

Menurut Akik Hidayat dan Tuty Alawiyah yang berjudul Enskripsi dan Deskripsi teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks persegi panjang, pada jurnal ini penulis menggunakan modulo 95 artinya inputan data ada 95 simbol. Untuk memudahkan perhitungan pada saat inisalisasi matriks kunci, proses enkripsi dan proses deskripsi menggunakan program aplikasi C++[3].

Tujuan dari pembahasan ini ingin memberikan gambaran bahwa matakuliah matriks bisa dipakai dalam matakuliah lain yang berhubungan dengan komputer. Aplikasi matrik ini dicari dengan enggunakan program Matlab.

2. METODE PENELITIAN

Metode Penelitian pada penyusunan ini terdiri atas studi pustaka yaitu mengumpulkan bahan-bahan referensi baik buku, artikel, makalah maupun situs internet mengenai algoritma kriptograpy Hill Cipher. Dalam ilmu kriptografi, pesan atau data terlebih dahulu dikirim dalam bentuk kode-kode yang dikenal dengan enskripsi. Kemudian enskripsi diartikan sebagai proses diubah nya data atau pesan yang hendak dikirim yang menjadi bentuk yang tidak bisa dikenali oleh pihak ketiga. Setelah data atau pesan tersebut sampai kepihak penerima, maka pihak penerima akan melakukan deskripsi yang merupakan kebalikan dari enskripsi. Deskripsi diartikan sebagai proses mengubah data atau pesan kembali kebentuk semula sehingga data atau pesan dapat tersampaikan dan dimengerti oleh penerima. Data atau pesan asli nama Plaintext (data yang dibaca) sedangkan dikodekan dinamakan Chipertext (data yang di enskripsikan). Proses enkripsi dan deskripsi memerlukan kunci dalam mekanismenya dan biasanya berupa string atau deretan bilangan[2].



Gambar 2. 1 Skema Enskripsi dan Deskripsi dengan menggunakan Kunci

3. HASIL DAN PEMBAHASAN

1. Metode Hill Cipher

Hill Cipter termasuk dalam salah satu kriptosistem Polialfabetik, artinya setiap karakter alphabet bisa dipetakkan ke lebih dari satu macam karakter alphabet [8]. Sebelum lanjut ke proses enkripsi dan deskripsi berikut table konversi setiap huruf alphabet ke dalam bilangan bulat.

Jurnal KomtekInfo, Vol.8 No.2Tahun 2021
e-ISSN: 2502-8758|| p-ISSN : 2356-0010
DOI: 10.35134/komtekinfo.v7i4
Page :154-162

Tabel 3.1 Konveksi alphabet ke dalam bilangan bulat

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z	.	,	?	!
20	21	22	23	24	25	26	27	28	29

2. Membuat teks asli (plaintext) yang dikonversikan tiap-tiap huruf alphabet kedalam sebuah bilangan 0 sampai 30. Kemudian masukan kepersamaan matrik.

Definisi matriks adalah susunan segi empat siku-siku dari bilangan-bilangan. Bilangan-bilangan dalam susunan tersebut dinamakan entri dalam matriks. Secara umum matriks P adalah matriks *mxn* sehingga dapat dibuat persamaan matriks sebagai berikut[1]:

$$P = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \quad \ldots\ldots(1)$$

3. Proses Enkripsi

Enskripsi adalah proses mengubah suatu pesan asli (plaintext) menjadi pesan dalam kata sandi (ciphertext).

C = E . P …….. (1)

Ket :

C = proses dalam bahasa sandi (**C**iphertext)
E = Proses **E**nkripsi
P = Pesan Asli (**P**laintext)

4. Proses Deskripsi

Deskripsi adalah proses mengubah pesan asli dalam suatu bahasa sandi menjadi pesan asli kembali sehingga dapat dibaca dan dimengerti.

P = D . C …… (2)

Ket :

P = pesan asli (**P**laintext)
D = Proses **D**eskripsi
C = proses dalam bahasa sandi (**C**iphertext)

5. Memilih matriks kunci dengan ordo tergantung pada kolom yang terdapat pada matriks awal.

Syaratnya pada kunci matriks harus memiliki invers, disini dipilih kunci ordo 4x4, kunci pada matriks ini disesuaikan dengan kolom pada matriks plaintext, misalnya plaintextnya ukuran mxn, maka kuncinya harus berordo nxn. Ukuran n yang kita peroleh kita dapat dari ukuran kolom pada plaintext.

Sesuai dengan prinsif perkalian matriks “Definisi: jika A adalah matriks mxr dan B adalah matriks rxn, maka hasil kali AB adalah matriks mxn yang entri-entrinya ditentukan sebagai berikut. Untuk mencari entri dalam baris i dan kolom j dari AB, pilihlah baris I dari matriks A dan kolom j dari matriks B. kalikanlah entri-entri yang bersesuaian dari baris dan kolom tersebut bersama-sama dan kemudian tambahkanlah hail kali yang dihasilkan”[3].

Jurnal KomtekInfo, Vol.8 No.2Tahun 2021
e-ISSN: 2502-8758|| p-ISSN : 2356-0010
DOI: 10.35134/komtekinfo.v7i4
Page :154-162

6. Perkalian matriks dan invers matrik menggunakan aplikasi matlab.

Selain karakter khusus dan fungsi yang telah dijelaskan digunakan operasi matriks dan operasi elemen.

Tabel 3.2 Operasi matriks dan operasi elemen

Operasi matriks	Penjelasan matematis	Operasi elemen	Penjelasan matematis
+	C = A + B $c_{ij} = a_{ij} + b_{ij}$	+	C = A + B $c_{ij} = a_{ij} + b_{ij}$
-	D = A – B $d_{ij} = a_{ij} - b_{ij}$	-	D = A – B $d_{ij} = a_{ij} - b_{ij}$
*	C = A * B $C_{ij} = \sum_k a_{ik} b_{ik}$	.*	D = A. * B $C_{ij} = a_{ij} .* b_{ij}$
^	B = A*3 = A*A*A	.^	B = A*3 $b_{ij} = a_{ij}^n$
‘	W = Z’ $W_{ij} = \overline{Z_{ij}}$	.‘	W = Z.’’ $W_{ij} = \overline{Z_{ij}}$
/	Jika A^{-1} ada, maka B/A = B/A^{-1}	./	C = B./A $C_{ij} = b_{ij}/a_{ij}$, $a_{ij} \neq 0$
\	Jika A^{-1} ada, maka A\B = A^{-1}*B	.\	C = A.\B $C_{ij} = b_{ij}/a_{ij}$, $a_{ij} \neq 0$

Contoh :

STOPPENYEBARANVIRUS.

1. Konversi Plaintext kedalam huruf

S 18	T 19	O 14	P 15
P 15	E 4	N 13	Y 24
E 4	B 1	A 0	R 17
A 0	N 13	V 21	I 8
R 17	U 20	S 18	. 26

2. Matriks Plaintext

$$P = \begin{bmatrix} 18 & 19 & 14 & 15 \\ 15 & 4 & 13 & 24 \\ 4 & 1 & 0 & 17 \\ 0 & 13 & 21 & 8 \\ 17 & 20 & 18 & 26 \end{bmatrix}_{5x4}$$

Pada plaintextnya dapat dibuat matriks yang berukuran 5x4,maka kunci matriks yang dibuat disesuaikan dengan dengan banyaknya kolom pada matriks P yaitu 4 kolom, maka matriks kuncinya 4x4. Dengan syarat matriks kuncinya harus memiliki determinan atau D ≠ 0. Aplikasi matlab: Pada aplikasi matlab diawal dan diakhir dikasih kurung siku dan tiap baris pada matriks dibatasi oleh titik koma(;):

```
>> P=[18 19 14 15;15 4 13 24; 4 1 0 17;0 13 21 8; 17 20 18 26]

P =

    18    19    14    15
    15     4    13    24
     4     1     0    17
     0    13    21     8
    17    20    18    26
```

3. Tentukan kunci dengan ordo 4x4

Pada matriks kunci atau proses enskrip ordo matriknya diambil dari kolom pada matrik P, dimana baris tersebut dibuat matriks persegi. Sedangkan elemen dari matriks dibuat bebas. Kunci ini yang harus dijaga biar tidak bocor kepihak ketiga. Kunci matriks yang dibuat adalah sebagai berikut:

$$E = \begin{bmatrix} 1 & 2 & 2 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 3 & 4 & 5 \\ 1 & 1 & 1 & 2 \end{bmatrix}$$

Tampilan dimatlab seperti berikut:

```
>> E=[1 2 2 1 ;1 2 3 1 ;1 3 4 5 ; 1 1 1 2 ]

E =

     1     2     2     1
     1     2     3     1
     1     3     4     5
     1     1     1     2
```

4. Proses Enskripsi

Proses dalam bahasa sandi (**C**iphertext). Untuk memperoleh proses ciphertext didapatkan perkalian matriks pada enskripsi dan plaintext.

C = E . P

$$C = \begin{bmatrix} 18 & 19 & 14 & 15 \\ 15 & 4 & 13 & 24 \\ 4 & 1 & 0 & 17 \\ 0 & 13 & 21 & 8 \\ 17 & 20 & 18 & 26 \end{bmatrix} x \begin{bmatrix} 1 & 2 & 2 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 3 & 4 & 5 \\ 1 & 1 & 1 & 2 \end{bmatrix}$$

Aplikasi Matlab:

Operasi yang dipakai pada matlab yaitu operasi perkalian matriks yang ditandai dengan

C = P*E sesuai dengan persamaan (1).

```
>> C=P*E

C =

   66.0000  131.0000  164.0000  137.0000
   56.0000  101.0000  118.0000  132.0000
   22.0000   27.0000   28.0000   39.0000
   42.0000   97.0000  131.0000  134.0000
   81.0000  154.0000  192.0000  179.0000
```

Didapatkan kode rahasia (**C**iphertext) yaitu:

66 131 164 137
46 101 118 132
22 27 28 39
42 97 131 134
81 154 192 179

Pesan dalam bentuk angka ini yang akan dikirim kepenerima pesan. Cara membaca pesan yang terkirim

5. Pesan yang didapatkan merupakan **C**iphertext yaitu pesan dalam bentuk sandi.

Perkalian matriks **P**laintext atau pesan asli dengan invers matrik kunci. Matriks kunci dicari inversnya kemudian dikalikan dengan matrik (**C**iphertext).

Matriks kunci

$$E = \begin{bmatrix} 1 & 2 & 2 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 3 & 4 & 5 \\ 1 & 1 & 1 & 2 \end{bmatrix}$$

Maka Invernya dari matriks kunci menggunakan operasi matlab yaitu inv(E):

```
>> D=inv(E)

D =

   -0.4000    0.6000   -0.6000    1.4000
    1.8000   -1.2000    0.2000   -0.8000
   -1.0000    1.0000         0         0
   -0.2000   -0.2000    0.2000    0.2000
```

Kemudian matrik **C**iphertext dikalikan dengan invers dari matrik (E) atau dengan rumus P = D . C sesuai dengan persamaan kedua, maka diperoleh tampilan dalam matlab adalah:

```
>> P=C*D

P =

   18.0000   19.0000   14.0000   15.0000
   15.0000    4.0000   13.0000   24.0000
    4.0000    1.0000    0.0000   17.0000
   -0.0000   13.0000   21.0000    8.0000
   17.0000   20.0000   18.0000   26.0000

>>
```

Maka hasil didapatkan kedalam matriks plaintext atau kata sandi yang asli, maka tampilan yaitu :

18 19 14 15
15 4 13 24
4 1 0 17
0 13 21 8
17 20 18 26

Dikonversikan kedalam huruf akan terbentuk:

"STOPPENYEBARABVIRUS"

SIMPULAN

Pada kesempatan ini matrik dapat diaplikasi keilmu kriptografi dengan mengunakan operasi pada matrik yaitu perkalian matriks dan invers matriks dengan menggunakan matlab. Berapa pun ordo yang dipakai dalam operasi matriks dan invers matriks akan lebih gampang mencarinya solusinya dengan mengunakan software matlab.

UCAPAN TERIMAKASIH

Terimakasih kepada Universitas Putra Indonesia yang telah bersedia menampung karya ilmiah penulis untuk diterbitkan di LLPM UPI YPTK Padang. Serta juga tidak lupa ucapan terimakasi kepada ketua dan staff LPPM yang bersedia dan menyempatkan untuk membaca tulisan penulis ini.

DAFTAR PUSTAKA

[1]. Adiwijaya. 2014. Aplikasi Matriks dan Ruang Vektor. Yogyakarta: Graha Ilmu.

[2]. Amin, M. M. (2016). Komunikasi Berbasis Teks. *Jurnal Pseudocode*, *III*(September), 129–136.

[3]. Anton, howard.1987. Aljabar Liner Elementer. Bandung: Erlangga

[4]. Hidayat, A., & Alawiyah, T. (2013). Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang. *Jurnal Matematika Integratif*, *9*(1), 39. https://doi.org/10.24198/jmi.v9i1.10196

[5]. Ilmu, B., & Dan, I. (n.d.). Pengembangan Kurikulum

[6]. It, S. P. K. (n.d.). *Teori&aplikasi*.

[7]. Sumandri. (2017). Studi Model Algoritma Kriptografi Klasik dan Modern. *Seminar Matematika Dan Pendidikan Matematika UNY*, 265–272.

[8]. Wardani, I. E. (2015). Pemecahan Sandi Kriptografi dengan Menggabungkan Metode Hill Cipher dan Metode Caesar Chipher. *Cauchy*, *2*(4), 232. https://doi.org/10.18860/ca.v2i4.3120