Aplikasi Matriks Dalam Mengirim dan Membaca Suatu Pesan Kriptografi

(Drs. Emut, M.Si)
Dosen Jurusan Pendidikan Matematika FMIPA UNY

I. Pendahuluan

Dalam dunia kriptografi ternyata huruf yang sama pada pesan mempunyai image huruf yang sama juga. Hal ini mempunyai tingkat resiko yang tinggi karena mudah ditebak. Untuk menyelesaikan hal ini maka pesan haruslah disandikan(*encoding*). Tujuan membuat *encoding* adalah aman dari para pembongkar sandi sehingga hanya penerima saja yang mengetahui isinya.

Pesan dikemas dan ditulis dalam bentuk barisan bilangan atau huruf tidak beraturan. Pesan sandi yang dikirim merupakan hasil pengolahan dan pemrosesan dengan satu atau lebih operasi matriks. Tingkat keamanan suatu pesan tergantung pada kompleksitas pemrosesan operasi matriks yang digunakan.

Pada proses pengiriman pesan, sender(pengirim) menyertakan juga perangkat yang digunakan untuk mengolah/merubah pesan. Perangkat yang dimaksud adalah aturan konversi dan matriks pemrosesnya (matriks kunci). Berdasarkan ketiga perangkat inilah receiver (penerima) dapat membongkar/membaca makna pesan yang dikirim.

Pada tulisan ini akan dibahas proses pengiriman dan pembacaan suatu pesan sandi yang sangat sederhana. Diharapkan dapat digunakan sebagai ilustrasi untuk mengembangkan peran matriks dan matriks invers dalam dunia persandian (kriptografi).

II. Kriptografi

Kriptografi adalah suatu ilmu yang membahas tentang persandian. Kriptografi meliputi penentuan pesan, proses persandian dan pembongkaran pesan sandi. Proses persandian (*encoding*) diawali dengan menentukan aturan konversi, matriks kunci dan perkalian kedua matriks tersebut. Hal ini dimaksudkan agar pesan tidak bisa diketahui maknanya kecuali penerima pesan(*receiver*). Kualifikasi keamanan suatu pesan sandi ditentukan oleh kompleksitas aturan konversi dan pemilihan matriks kunci. Akibatnya, semakin kompleks aturan konversi dan matriks kunci akan menghasilkan pesan sandi yang lebih aman.

Dalam pembahasan ini, akan dikaji tentang mengirim pesan sandi dan membaca person serta beberapa contoh untuk memperkuat pemahaman.

2. 1 Mengirim Pesan

◆Langkah-langkah mengirim pesan

1. **Tulis pesan Anda [dalam deretan huruf yang bermakna]**
2. **Tentukan “**aturan konversi**” yang Anda gunakan**

Misal,	**A,**	**B,**	**C, …,**	**Z,**	**_,**	**, ,**	**.,**	**?,**	**!,**
	↕	↕	↕		↕				↕
	1,	**2,**	**3,…,**	**26,**	**27,**	**28,**	**29,**	**30,**	**31**

3. **Tulis pesan (1) dalam bentuk konversi**
4. **Tulis pesan (3) dalam bentuk matriks, misal** M
5. **Tentukan matriks kunci** A**, dengan kriteria sbb:**

- **Semua unsur dari matriks A dan A^{-1} adalah bulat**
- **Matriks A dan M dapat dikalikan(multiplicable)**

6. **Tentukan matriks** P**, dengan** P = AM
7. **Tulis matriks** P **dalam deretan bilangan. [P inilah pesan yang dikirim]**

Dalam proses pengiriman pesan khusus tersebut, seorang penerima (receiver) akan menerima beberapa perangkat. Perangkat yang disertakan digunakan untuk membongkar /membaca pesan yang dikirimkan.

Perangkat tersebut adalah :

- **Pesan dalam deretan bilangan [pesan (7)]**
- **Aturan konversi [pesan (2)]**
- **Matriks kunci [pesan (5)].**

◆**Contoh**.

Seseorang mengirim pesan kepada sahabatnya. Pesan tersebut adalah "**BE SELF FOREVER.**", sehingga dia tidak keluar dari jati dirinya. Agar tidak menyinggung perasaan orang yang membaca dan lebih menarik maka pesannya dikirim dalam sandi.

◆**Langkah-langkahnya, adalah sbb:**

1. Pesan : **BE SELF FOREVER.**
2. Aturan konversi :

A,	**B**,	**C**, …, **Z**,	_,	, ,	**.**,	**?**,	**!**,
↕	↕	↕	↕	↕	↕	↕	↕
1,	**2**,	**3**,…,	**26**,	**27**,	**28**,	**29**,	**30**,	**31**

3. Pesan (1) menjadi : 2 5 27 19 5 12 6 27 6 15 18 5 22 5 18 29
4. Tulis pesan (3) dalam matriks,

$$M_{2x8} = \begin{bmatrix} 2 & 5 & 27 & 19 & 5 & 12 & 6 & 27 \\ 6 & 15 & 18 & 5 & 22 & 5 & 18 & 29 \end{bmatrix}$$

◆Perhatian. Ukuran matriks M bergantung pada ukuran matriks kunci A. Ukuran M adalah (**2**x…), angka **2** mengacu pada ukuran A, yaitu **2**x**2**.

5. Misalkan diberikan matriks kunci A, dengan $A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$.

   ♦Ingat, bahwa semua unsur dari A dan unsur A^{-1} adalah bulat. Hal itu dapat dilakukan (salah satunya) dengan membuat det(A)=1.

6. Misalkan P, dengan P = AM maka diperoleh

$$P = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 5 & 27 & 19 & 5 & 12 & 6 & 27 \\ 6 & 15 & 18 & 5 & 22 & 5 & 18 & 29 \end{bmatrix}$$

$$= \begin{bmatrix} 4+18 & 10+45 & 54+54 & 38+15 & 10+66 & 24+15 & 12+54 & 54+87 \\ 2+12 & 5+30 & 27+36 & 19+10 & 5+44 & 12+10 & 6+36 & 27+58 \end{bmatrix}$$

$$= \begin{bmatrix} 22 & 55 & 108 & 53 & 76 & 39 & 66 & 141 \\ 14 & 35 & 63 & 29 & 49 & 22 & 42 & 85 \end{bmatrix}$$

7. Pesan akhir yang didapat adalah

22 55 108 53 76 39 66 141 14 35 63 29 49 22 42 85

◆Perangkat yang dikirim terdiri 3 hal yaitu :

1. **pesan** : **22 55 108 53 76 39 66 141 14 35 63 29 49 22 42 85**

2. aturan konversi :

A,	B,	C, …, Z,	_,	, ,	.,	?,	!,
↕	↕	↕	↕	↕	↕	↕	↕
1,	2,	3,…,	26,	27,	28,	29,	30,	31

3. **matriks kunci A**,

$$A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

2.2. Membaca Isi Pesan

Seseorang mengirim pesan mengharapkan pesan tersebut dapat dibaca sehingga isi pesan segera diketahui oleh penerima. Maka penulisan alamat, bahasa dan teknik penulisan sangatlah penting untuk diketahui kedua pihak. Khusus teknik penulisan pesan, disamping faham cara membaca juga diberi fasilitas untuk membongkarnya. Dalam membaca suatu pesan sandi, penentuan matriks balikan dari matriks kunci menjadi langkah pokok.

◆**Langkah-langkah membaca pesan**

1. **Tulis pesan yang diterima dalam bentuk matriks**, misal P. Ukuran P multiplicable dengan matriks A^{-1} artinya matriks A^{-1} dan matriks P dapat dikalikan. [ingat : ukuran matriks A^{-1} = ukuran matriks A]
2. **Tentukan A^{-1}** (dengan menggunakan metode yang telah diketahui)
3. **Tentukan $M = A^{-1} P$**. [karena $A^{-1} P = A^{-1} (AM) = (A^{-1}.A) M = I. M = M$]
4. **Tulis M dalam bentuk deretan bilangan**
5. **Tulis konversi dari (4) dengan aturan konversi**
6. **Tulis pesan yang dimaksud**.

◆**Contoh 1.** Anda perhatikan contoh pada 4.2. Kita akan membaca pesan yang dikirim dari contoh tersebut. Perangkat yang dikirim

1. pesan : **22 55 108 53 76 39 66 141 14 35 63 29 49 22 42 85**

2. aturan konversi :

A,	B,	C, …,	Z,	_,	, ,	.,	?,	!,
↕	↕	↕	↕	↕	↕	↕	↕	↕
1,	2,	3,…,	26,	27,	28,	29,	30,	31

3. matriks kunci A,

$$A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

Kita akan membaca pesan yang dikirim berdasarkan petunjuk **langkah-langkah** di atas.

1. Tulis pesan dalam matriks P, yaitu

$$P = \begin{bmatrix} 22 & 55 & 108 & 53 & 76 & 39 & 66 & 141 \\ 14 & 35 & 63 & 29 & 49 & 22 & 42 & 85 \end{bmatrix}$$

2. Mencari A^{-1}.

Karena $A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$ maka didapat $A^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$

3. Mencari

$$M = A^{-1} P = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 22 & 55 & 108 & 53 & 76 & 39 & 66 & 141 \\ 14 & 35 & 63 & 29 & 49 & 22 & 42 & 85 \end{bmatrix}$$

$$\begin{bmatrix} 44-42 & 110-105 & 216-189 & 106-87 & 152-147 & 78-66 & 132-126 & 282-255 \\ -22+28 & -55+70 & -108+126 & -53+58 & -76+98 & -39+44 & -66+84 & -141+170 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 5 & 27 & 19 & 5 & 12 & 6 & 27 \\ 6 & 15 & 18 & 5 & 22 & 5 & 18 & 29 \end{bmatrix}$$

4. Menulis pesan P dalam deretan bilangan, yaitu :

2 5 27 19 5 12 6 27 6 15 18 5
22 18 29

5. Tulis pesan dalam bentuk konversi yang dikirim, yaitu :

B E _S E L F _ F O R E V E R .

6. Pesan yang dikirim adalah : **BE SELF FOREVER**.

◆**Contoh 2**. Seorang teman mengirim pesan/nasehat kepada Anda dalam bentuk sandi. Dia sangat mengharapkan Anda dapat membaca dan merealisasikan dalam kehidupan sehari-hari. Disamping mengirim pesan dia juga mengikutkan perangkat (fasilitas) untuk membacanya. Pesan dan perangkat yang dikirim adalah sebagai berikut :

1. Pesan :
   32 31 45 18 41 32 32 79 44 47 23 25 27 12 27
2. Aturan Konversi :

A,	B,	C, …,	Z,	_,
↕	↕	↕	↕	↕
1,	2,	3,…,	26,	0

dan

f(X*)=(X*+5) mod 27, dengan X* huruf alphabet.

(contoh : f(A)=(A+5) mod 27 ⇨ f(1)=(1+5) mod 27 = 6,

f(D)=(D+5) mod 27 ⇨ f(4)=(4+5) mod 27 = 9,

f(X)=(X+5) mod 27 ⇨ f(24)=(24+5) mod 27 = 2, dst)

3.Matriks kunci A, dengan

$$A = \begin{bmatrix} 2 & 0 & 1 \\ 3 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

♦**Penyelesaian** : Langkah-langkah yang dilakukan untuk membaca pesan terse-but, adalah :

1. Tulis pesan dalam matriks P dengan mengingat ukuran A. Karena A(3x3) maka ukuran P adalah 3x5, yaitu data pesan dibagi tiga baris. Matriks P adalah

$$P = \begin{bmatrix} 32 & 31 & 45 & 18 & 41 \\ 32 & 32 & 79 & 44 & 47 \\ 23 & 25 & 27 & 12 & 27 \end{bmatrix}$$

2. Menentukan matriks A^{-1} dengan menggunakan metode Adjoint, yaitu A^{-1} = Adj A / |A|.

Karena $A = \begin{bmatrix} 2 & 0 & 1 \\ 3 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$ maka dengan menggunakan perluasan baris –1, didapat

$$\text{Det}(A) = a_{11} M_{11} - a_{12} M_{12} + a_{13} M_{13}$$
$$= 2\,(1\text{-}0) - 0\,(3\text{-}0) + 1\,(0\text{-}1)$$
$$= 2 - 0 + 1(-1) = 1$$

$$\text{Adj A} = \begin{bmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{bmatrix}, \text{(mohon diperhatikan unsur-unsurnya)}$$

Diperoleh

$A_{11} = + M_{11} = (1\text{-}0) = 1$
$A_{21} = - M_{21} = -(0\text{-}0) = 0,$
$A_{31} = + M_{31} = (0\text{-}1) = -1$
$A_{12} = - M_{12} = -(3\text{-}0) = -3$
$A_{22} = + M_{22} = (2\text{-}1) = 1,$
$A_{32} = - M_{32} = -(0\text{-}3) = 3$
$A_{13} = + M_{13} = (0\text{-}1) = -1$
$A_{23} = - M_{23} = -(0\text{-}0) = 0$
$A_{33} = + M_{33} = (2\text{-}0) = 2.$

Maka didapat

$$\text{Adj A} = \begin{bmatrix} 1 & 0 & -1 \\ -3 & 1 & 3 \\ -1 & 0 & 2 \end{bmatrix} \text{ sehingga menurut rumus diperoleh}$$

$$A^{-1} = \text{Adj A} / \det(A) = \begin{bmatrix} 1 & 0 & -1 \\ -3 & 1 & 3 \\ -1 & 0 & 2 \end{bmatrix} / 1 = \begin{bmatrix} 1 & 0 & -1 \\ -3 & 1 & 3 \\ -1 & 0 & 2 \end{bmatrix}$$

3. Menentukan matriks M, yaitu :

$$M = A^{-1} * P = \begin{bmatrix} 1 & 0 & -1 \\ -3 & 1 & 3 \\ -1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 32 & 31 & 45 & 18 & 41 \\ 32 & 32 & 79 & 44 & 47 \\ 23 & 25 & 27 & 12 & 27 \end{bmatrix}$$

4. $M = A^{-1} * P =$

$$\begin{bmatrix} (1.32 + 0.32 + (-1.23)) & (1.31 + 0.32 + (-1.25)) & 18 & 6 & 14 \\ 5 & 14 & 25 & 26 & 5 \\ 14 & 19 & 9 & 6 & 13 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & 6 & 18 & 6 & 14 \\ 5 & 14 & 25 & 26 & 5 \\ 14 & 19 & 9 & 6 & 13 \end{bmatrix}$$

2. Pesan M pada (4), disusun membentuk deretan bilangan, yaitu :
   9 6 18 6 14 5 14 25 26 5 14 19 9 6 13

5. Pesan pada (5), dikonversi dengan menggunakan Aturan Konversi, didapat :
   9 = 9 mod 27 = (4+5)mod 27 shg 9 $\rightarrow$ 4 yaitu D
   6 = 6 mod 27 = (1+5)mod 27 shg 6 $\rightarrow$ 1 yaitu A
   18 =18 mod 27 = (13+5) mod 27 shg 18 $\rightarrow$13 yaitu M,
   6 = 6 mod 27 = (1+5)mod 27 shg 6 $\rightarrow$ 1 yaitu A
   14 = 14 mod 27 = (9+5)mod 27 shg 14 $\rightarrow$ 9 yaitu I,
   dan seterusnya.

   Sehingga didapat pesan
D A M A I _ I T U _ I N D A H

3. Pesan yang dimaksud adalah : **DAMAI ITU INDAH**

III. Kesimpulan

Berdasarkan pembahasan dapat disimpulkan sebagai berikut

1. Matriks memberikan tingkat keamanan yang tinggi dalam mengirim suatu pesan sandi
2. Tingkat keamanan suatu pesan sandi ditentukan oleh kompleksitas aturan konversi dan matriks kunci yang digunakan.