Implementasi Matriks dalam Kriptografi

Aditio Pangestu 13514030
Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
Aditio_pangestu@itb.ac.id

***Abstrak*—Makalah ini menjelaskan bagaimana suatu matriks dapat diimplementasikan dalam ilmu kriptografi. Secara spesifik penerapan matriks lebih kepada sebagai kunci dalam proses ekripsi dan dekripsi. Penerapan matriks tersebut berupa perkalian matriks dan matriks invers.**

***Kata kunci*—Matriks, Kriptografi, Enkripsi, Dekripsi.**

I. PENDAHULUAN

Kriprografi merupakan cabang ilmu yang mepelajari penjagaan sebuah pesan yang rahasia dengan mengubahnya ke suatu bentuk yang tidak bermakna. Kriptografi berasal dari Bahasa Yunani yang memiliki sinonim yaitu pesan rahasia. Kriptografi juga merupakan ilmu yang sangat penting untuk masa sekarang sebab kriptografi dapat menjaga suatu pesan yang tidak ingin diketahui oleh pihak-pihak tertentu. Salah satu contoh dari pesan tersebut adalah password.

Perkembangan kriptografi sendiri sudah cukup luas. Sudah banyak ilmu-ilmu yang dapat diterapkan dalam kriptografi. Salah satu pengetahuannya yaitu invers dari sebuah matriks. Pada makalah ini akan dibahas penerepan invers dari sebuah matriks dalam kriptografi.

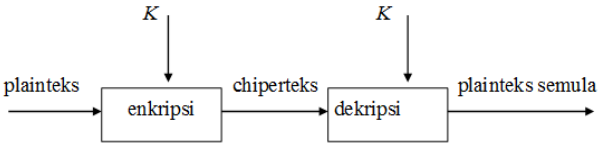
II. DASAR TEORI

Ilmu dasar yang akan dibahas pada makalah ini yaitu ilmu dasar mengenai kriprografi dan matriks yang merupakan cabang ilmu dari aljabar geometri.

2.1 Kriptografi

Dalam sub-bab ini akan dibahas beberapa istilah yang akan digunakan dalam makalah ini yaitu :

a. Pesan / Plainteks : sebuah informasi yang dapat dimengerti maknanya. Contoh : ini plainteks.
b. Cipherteks : sebuah informasi yang telah disandikan sehingga sulit untuk mengerti maknanya. Contoh : joj qmbjolr.
c. Enkripsi : sebuah proses mengubah plainteks menjadi cipherteks.
d. Dekripsi : sebuah proses mengubah chiperteks menjadi plainteks



Gambar 1. Proses Enkripsi dan Dekripsi

Dari gambar 1, diperlukan K untuk melakukan proses enkripsi dan dekripsi. Istilah dari K tersebut adalah kunci. Kunci dalam proses tersebut beragam, dalam makalah ini kunci dari proses enkripsi dan dekripsi berupa sebuah matriks dan beberapa informasi.

2.2 Matriks

Matriks merupakan kumpulan suatu informasi dalam bentuk segi empat yang tersusun dalam baris dan kolom. Berikut notasi matriks A_{bxk} yang memiliki ukuran bxk secara umum,

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{b1} & \cdots & a_{bk} \end{bmatrix}$$

A. Jenis-Jenis Matriks

Ada berbagai jenis matriks berdasarkan elemen penyusun dan ukuran kolom dan baris. Pada makalah ini akan dibahas dua jenis matriks.

1. Matriks persegi merupakan matriks yang memiliki ukuran kolom sama dengan ukuran baris. Dengan kata lain, matriks ini memiliki ukuran NxN. Contoh: Matriks persegi A berukuran 3x3

$$A = \begin{bmatrix} 1 & 2 & 4 \\ 5 & 3 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

2. Matriks identitas merupakan matriks persegi yang susunan elemen-elemen diagonal adalah angka 1 dan elemen lainnya berupa angka 0. Matriks identitas dinotasikan dengan I.

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

B. Operasi Matriks

2.2.2.1 Jenis Operasi

Ada berbagai jenis operasi matriks. Pada makalah ini hanya dibahas dua jenis operasi matriks yaitu

1. Operasi Perkalian Matriks dengan Matriks
   Misalkan A_{bxk} dan B_{qxp} merupakan matriks. Agar dapat melakukan operasi perkalian pada kedua matriks tersebut (A_{bxk} x B_{qxp}) harus dipenuhi sebuah syarat yaitu nilai k = q. Contoh :
   A = $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dan B = $\begin{bmatrix} e \\ f \end{bmatrix}$ sehingga C = AxB
   C = $\begin{bmatrix} axe + bxf \\ cxe + dxf \end{bmatrix}$

2. Operasi Baris Elementer (OBE)
   OBE merupakan operasi penambahan atau perkalian yang dilakukan pada suatu baris dari matriks. Operasi baris elementer meliputi :
   a. Pertukaran baris.
   b. Perkalian suatu baris dengan suatu konstanta bukan 0.
   c. Penjumlahan hasil perkalian suatu baris dengan konstanta bukan nol dengan suatu baris yang lain.

   Contoh[1] :

   Pertukaran baris :

$$A = \begin{pmatrix} -3 & -2 & -1 \\ 1 & 2 & 3 \\ 0 & 2 & 4 \end{pmatrix} \; b_1 \leftrightarrow b_2 \sim \begin{pmatrix} 1 & 2 & 3 \\ -3 & -2 & -1 \\ 0 & 2 & 4 \end{pmatrix}$$

   Operasi antar baris :

$$A = \begin{pmatrix} 1 & -1 & 0 & -1 \\ 0 & 2 & 1 & 7 \\ 2 & -1 & 1 & 3 \end{pmatrix} \; -2b_1 + b_3 \sim \begin{pmatrix} 1 & -1 & 0 & -1 \\ 0 & 2 & 1 & 7 \\ 0 & 1 & 1 & 5 \end{pmatrix}$$

2.2.2.2 Sifat Operasi

Ada beberapa sifat dari operasi matriks yang harus diketahui pada makalah ini yaitu :

1. Asosiatif
   Ax(BxC) = (AxB)xC
2. Komutatif
   AxB ≠ BxA

C. Matriks Invers

Misalkan A dan B merupakan matriks persegi serta I merupakan matriks identitas. Jika AxB = I maka B dikatakan sebagai matriks invers dari A, sebaliknya A juga dapat dikatakan sebagai matriks invers dari B. Notasi dari matriks invers adalah A^{-1}. Contoh B merupakan matriks invers dari A, maka didapat B = A^{-1}.

Untuk mendapatkan matriks invers dapat dicari mengguanakan matriks elementer, yaitu[1] :

$$(A \mid I) \sim (I \mid A^{-1})$$

Matriks A pada ruas kiri dikenakan operasi baris elementer secara bersamaan dengan matriks I pada ruas kanan sehingga matriks A menjadi matriks identitas dan matriks I menjadi matriks invers dari A. Bila saat melakukan OBE ditemukan baris A yang seluruh elemennya bilangan 0, maka matriks tersebut tidak memiliki matriks invers. Matriks tersebut dikatakan sebagai matriks singular.

Contoh[1] :

Akan dicari invers matriks dari A = $\begin{bmatrix} 3 & 2 & -1 \\ 1 & 1 & 0 \\ -2 & -2 & 1 \end{bmatrix}$

dengan menggunakan OBE.

$$\left(\begin{array}{ccc|ccc} 3 & 2 & -1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ -2 & -2 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 1 & 0 \\ 3 & 2 & -1 & 1 & 0 & 0 \\ -2 & -2 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & -1 & -1 & 1 & -3 & 0 \\ 0 & 0 & 1 & 0 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & -1 & 3 & 0 \\ 0 & 0 & 1 & 0 & 2 & 1 \end{array}\right)$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 & 2 & 1 \end{array}\right)$$

Jadi A^{-1} = $\begin{bmatrix} 1 & 0 & 1 \\ -1 & 1 & -1 \\ 0 & 2 & 1 \end{bmatrix}$

III. Aplikasi Matriks dalam Kriptografi

A. Enkripsi dengan sebuah Matriks

Untuk melaku enkripsi dengan sebuah matriks dibutuhkan beberapa tahap yaitu :

1. Ubahlah plainteks ke dalam sebuah angka.
   Proses pengubahan ini dilakukan per karakter. Kesesuain karakter dan angka dapat diatur sendiri. Dalam kasus ini, plainteks yang bisa di enkripsi memiliki lebih dari 4 karakter.
2. Susunlah angka-angka tersebut menjadi sebuah matriks.
   Matriks yang diharapkan memiliki baris dan kolom lebih dari 1 sebab matriks ini akan dikalikan dengan sebuah matriks persegi yang harus memiliki invers. Jika banyaknya angka berupa bilangan prima tambahkan sebuah angka yang tidak memiliki makna apa pun. Hal ini agar dapat disusun menjadi matriks yang memiliki lebih dari satu kolom dan baris. Ketersusunan angka di dalam matriks dibebaskan, tetapi agar lebih mudah dipahami, susunanan angka dapat berdasarkan kolom atau baris.
3. Kalikan matriks tersebut dengan sebuah matriks kunci.
   Matriks kunci merupakan matriks persegi yang memiliki ukuran yang sama dengan ukuran kolom dari matriks yang terbentuk dari plainteks. Matriks kunci juga harus memiliki invers.
4. Susunanlah elemen-elemen dari matriks hasil perkalian.
   Susunan dari elemen-elemennya disesuaikan dengan susunan angka-angka yang didapat dari plainteks ke matriks.

Contoh :

Akan dienkripsi kata berikut “ageometri” dalam beberapa tahap.

Tahap pertama, penyesuaian karakter dan angka dari kalimat diatas menggunakan pola sederhana yaitu a = 1, b =2, …, y = 25, dan z = 26. Sehingga didapat barisan angka dari kata “ageometri” adalah 1 7 5 15 13 5 20 18 9.

Tahap kedua, akan disusun angka-angka tersebut dalam sebuah matriks berukuruan 3x3 dengan susunan berdasarkan baris. Sehingga didapat matriks tersebut.

$$A = \begin{bmatrix} 1 & 7 & 4 \\ 15 & 13 & 5 \\ 20 & 18 & 9 \end{bmatrix}$$

Tahap ketiga, matriks kunci memiliki ukuran 3x3 karena ukuran kolom dari matriks diatas adalah 3. Sehingga didapat matriks kuncinya.

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

Lalu akan dikalikan kedua matriks di atas

$$C = BxA = \begin{bmatrix} 1 & 7 & 4 \\ 15 & 13 & 5 \\ 20 & 18 & 9 \end{bmatrix} x \begin{bmatrix} 3 & 2 & -1 \\ 1 & 1 & 0 \\ -2 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 13 & 29 & 16 \\ 16 & 20 & 10 \\ -12 & -22 & -11 \end{bmatrix}$$

Tahap keempat, dari matriks C didapat susunan angka yang baru : 13 29 16 16 20 10 -12 -22 -11.

Dari 4 tahap di atas didapat chiperteksnya adalah
13 29 16 16 20 10 -12 -22 -11.

B. Dekripsi dengan Sebuah Matriks

Untuk melaku dekripsi dengan sebuah matriks dibutuhkan beberapa tahap yaitu :

1. Susunanlah barisan angka dari chiperteks ke dalam matriks dengan ukuran kolom sama dengan ukuran kolom matriks kunci. Susunan yang dilakukan disesuakan dengan susunan saat Enkripsi.
2. Kalikan matriks tersebut dengan invers dari matriks kunci.
3. Susunan elemen-elemen matriks hasil perkalian kedalam barisan yang disesuaikan dengan penyusunan pada tahap 1.
4. Konversikan barisan angka menjadi sebuah plainteks kembali. Konversi disesuaikan dengan penyesuaian angka dan huruf diawal.

Contoh :

Akan didekripsi chiperteks berikut 13 29 16 16 20 10 -12 -22 -11 dalam beberapa tahap.

Tahap pertama, akan disusun angka-angka tersebut dalam sebuah matriks berukuruan 3x3 (ukuran kolom matriks kunci adalah 3) dengan susunan berdasarkan baris. Sehingga didapat matriks tersebut.

$$C = \begin{bmatrix} 13 & 29 & 16 \\ 16 & 20 & 10 \\ -12 & -22 & -11 \end{bmatrix}$$

Tahap kedua, kalikan matriks di atas dengan inversmatriks kunci. Invers dari matriks kunci adalah (Hasil didapat dari contoh Bab II)

$$B^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ -1 & 1 & -1 \\ 0 & 2 & 1 \end{bmatrix}$$

Lalu akan dikalikan kedua matriks di atas

$D = B^{-1}xC =$

$$\begin{bmatrix} 1 & 0 & 1 \\ -1 & 1 & -1 \\ 0 & 2 & 1 \end{bmatrix} x \begin{bmatrix} 13 & 29 & 16 \\ 16 & 20 & 10 \\ -12 & -22 & -11 \end{bmatrix} = \begin{bmatrix} 1 & 7 & 4 \\ 15 & 13 & 5 \\ 20 & 18 & 9 \end{bmatrix}$$

Tahap ketiga, dari matriks D didapat susunan barisannya adalah 1 7 5 15 13 5 20 18 9.

Tahap keempat, konversi dari barisan di atas adalah “ageometri”

Dari 4 tahap di atas didapat plainteksnya adalah “ageometri”. Proses ini dapat berhasil dilakukan karena pada proses ini memanfaatkan sifat dari invers matriks. Operasi di atas dapat dilihat sebagai berikut,

$D= B^{-1}xC = B^{-1}x(BxA) = (B^{-1}xB)xA = IxA = A$

IV. KESIMPULAN

Dalam melakukan enkripsi dan dekripsi ada 4 hal penting yang harus diperhatikan yaitu :

1. Skema pertukaran angka dengan karakter.
2. Susunan barisan angka ke dalam suatu matriks.
3. Matriks kunci yang memiliki invers.
4. Susunan elemen-elemen matriks ke dalam suatu barisan angka.

Dalan melakukan enkripsi dan dekripsi juga terdapat 3 faktor yang menentukan sebuah kunci yaitu :

1. Skema pertukaran angka ke dalam karakter
2. Susunan barisan angka ke dalam suatu matriks
3. Matriks kunci.

Dari 3 hal di atas didapat bahwa kunci dalam enkripsi dan dekripsi dengan menggunakan matriks sangat lah variatif.

V. CONCLUSION

Pada kesempatan ini, penulis mengucapkan terima kasih kepada Allah SWT atas segala kenikmatan yang telah diberikan baik berupa nikmat iman, kesehatan, maupun kekuatan dalam menyusun makalah ini. Penulis juga mengucapkan terima kasih kepada kedua orang tua penulis yang telah mendidik dan membesarkan penulis dengan penuh kasih sayang. Selanjutnya, penulis juga mengucapkan terima kasih kepada Bapak Judhi Sentosa. dan Bapak Rinaldi Munir selaku dosen pengajar mata kuliah Aljabar Geometri atas segala bimbingan serta ilmu yang telah diberikan kepada penulis. Tidak lupa penulis sampaikan pula rasa terima kasih kepada rekan-rekan penulis yang selalu mendukung, mendorong, serta

memberi semangat kepada penulis dalam menyelesaikan makalah ini. Terakhir, penulis juga menyampaikan terima kasih kepada seluruh pihak yang ikut membantu Makalah IF2123 Aljabar Geometri – Sem. I Tahun 2015/2016 pembuatan makalah ini baik yang secara langsung maupun tidak langsung.

REFERENCES

[1] Anonim, "Diktat kuliah Bab I – Matriks dan Operasinya", Unplubished.
[2] Munir, Rinaldi. "Matematika Diskrit", 2010, Penerbit Informatika.
[3] MacClelland, *Cryptography and Linear Algebra*. Unpublished.
[4] Neal, "Cryptography with Matrices," unpublished.
[5] Anonim, " Apllication of Invertible Matrices_Coding", http://www.sosmath.com/matrix/coding/coding.html, diakses pada 9 Desember 2015
[6] Houry, "Matrices Application to Cryptography" , http://aix1.uottawa.ca/~jkhoury/cryptography.htm , diakses pada 9 Desember 2015
[7] James, "Application of Matrices and Determinants", https://people.richland.edu/james/lecture/m116/matrices/applications.html , diakses pada Desember 2015.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 27 November 2013

Aditio Pangestu 13514030