Aplikasi Perkalian dan Invers Matriks dalam Kriptografi *Hill Cipher*

Catherine Pricilla-13514004
Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13514004@std.stei.itb.ac.id

***Abstrak*—Di era digital ini, pertukaran pesan di internet adalah hal yang sangat lazim dilakukan. Untuk melakukan pertukaran pesan melalui internet ini sebenarnya adalah hal yang cukup riskan karena pesan dapat dilihat atau diubah oleh orang lain yang sebenarnya tidak memiliki andil dalam pertukaran pesan tersebut. Oleh karena itu, menjaga kerahasiaan pesan sangat penting dilakukan. Kriptografi menjaga kerahasiaan suatu pesan. Pada makalah ini akan dibahas penggunaan matriks pada proses enkripsi dan dekripsi pada algoritma *Hill Cipher*.**

***Kata Kunci*—dekripsi, enkripsi, *Hill Cipher*, kriptografi, matriks**

I. PENDAHULUAN

Kriptografi adalah salah salah satu cabang ilmu informatika yang sebenarnya sudah ada dan digunakan sejak dahulu kala. Bahkan pada zaman sebelum masehi, kriptografi sudah diaplikasikan pada suatu alat bernama *scytale* di Yunani. Kriptografi juga digunakan pada zaman perang dunia kedua dengan mesin bernama Enigma yang digunakan oleh pihak Nazi Jerman untuk merahasiakan pesan-pesan dari sekutu. Tetapi akhirnya pihak sekutu berhasil memecahkan enkripsi tersebut sehingga memperpendek durasi dari perang dunia kedua.

Kriptografi digunakan oleh banyak kalangan seperti militer dan para pencinta, dahulu, para pencinta di India berkomunikasi menggunakan kriptografi agar pesan-pesan yang saling dikirimkan dan diterima tidak dapat dibaca oleh orang lain. Dengan kata lain, kriptografi sangat berperan penting dalam menjaga kerahasiaan dari suatu teks atau pesan.

Dalam dunia modern, kriptografi menjadi suatu hal yang dianggap sangat krusial. Sekarang, banyak sekali orang yang bertukar pesan dengan intensitas yang tinggi. Kriptografi menjadi sangat penting disebabkan oleh betapa pentingnya kerahasiaan suatu pesan dalam proses pengiriman dan penerimaan pesan, tetapi hal ini juga bersamaan dengan betapa rentannya suatu pesan itu untuk diubah atau dilihat oleh pihak ketiga yang tak seharusnya dapat melihat pesan tersebut. Dalam kemajuan teknologi internet, semua hal dilakukan dalam skala yang besar dan terhubung. Ini menyebabkan pengiriman pesan melalui internet menjadi sangat rentan untuk disadap oleh pihak ketiga, baik hanya untuk sekedar melihat atau untuk mengubah pesan tersebut. Bisa saja, pesan yang diberikan oleh pihak pertama kepada pihak kedua sudah berubah maknanya. Dengan kriptografi pengiriman pesan menjadi lebih aman karena sebelum mengirim pesan maka teks akan dienkripsi terlebih dahulu menjadi sandi-sandi sehingga untuk membacanya diperlukan untuk mendekripsi pesan-pesan tersebut.

Matriks yang merupakan salah satu pembahasan dalam aljabar linier adalah salah satu cara untuk mengenkripsi dan mengdekripsi suatu pesan. Penggunaan Algortima *Hill Cipher* melibatkan perkalian serta invers dari matriks untuk mengubah *plaintext* menjadi *ciphertext* dan mengubahnya kembali menjadi *plaintext* yang bisa diterima dan dibaca oleh pihak kedua.

II. LANDASAN TEORI

2.1 MATRIKS

2.1.1 Definisi Matriks

Matriks adalah susunan segi empat siku-siku dari bilangan yang dibatasi dengan tanda kurung.

Suatu matriks tersusun atas baris dan kolom, jika matriks tersusun atas *m* baris dan *n* kolom maka dikatakan matriks tersebut berukuran (berordo) *m* x *n*.

Penulisan matriks biasanya menggunakan huruf besar A, B, C dan seterusnya, sedangkan penulisan matriks beserta ukurannya (matriks dengan m baris dan n kolom) adalah A_{mxn}, B_{mxn} dan seterusnya.

Bentuk umum dari A_{mxn} adalah:

$$A_{mxn} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Dengan a_{ij} disebut sebagai elemen dari A yang terletak
pada baris ke-*i* dan kolom ke-*j*

2.1.2 Jenis-Jenis Matriks

Matriks sendiri terbagi menjadi beberapa jenis

diantaranya adalah:

1. Matriks Bujur Sangkar

   Matriks yang memiliki jumlah baris yang sama dengan jumlah kolomnya disebut sebagai matriks bujur sangkar. Pada matriks bujur sangkar terdapat elemen diagonal yang berjumlah n untuk matriks bujur sangkar yang berukuran nxn.

2. Matriks Diagonal

   Matriks yang memiliki elemen bukan diagonalnya bernilai nol disebut sebagai matriks diagonal. Tetapi elemen diagonalnya tidak diwajibkan bernilai 0.

   $A = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{bmatrix}$

3. Matriks Nol

   Matriks yang semua elemennya memiliki nilai 0 disebut sebagain matriks nol, matriks A merupakan contoh matriks nol.

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

4. Matriks Segitiga

   Matriks bujur sangkar dengan elemen-elemen yang dibawah atau diatas elemen diagonal bernilai nol disebut dengan matriks segitiga. Jika yang bernilai nol adalah elemen-elemen dibawah elemen diagonal maka disebut matriks segitiga atas, sebaliknya disebut matriks segitiga bawah. Tetapi elemen diagonalnya tidak diwajibkan bernilai 0.

   $A = \begin{bmatrix} 1 & 6 & 1 \\ 0 & 4 & 3 \\ 0 & 0 & 7 \end{bmatrix}$ $B = \begin{bmatrix} 1 & 0 & 0 \\ 6 & 4 & 0 \\ 7 & 8 & 7 \end{bmatrix}$ $C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 7 \end{bmatrix}$

   A merupakan contoh matriks segitiga bawah, B merupakan contoh matriks segitia atas, dan C merupakan matriks Matriks Identitas segitiga atas dan bawah.

5. Matriks Identitas

   Matriks identitas adalah matriks diagonal yang elemen diagonalnya bernilai 1, dan elemen bukan diagonalnya adalah 0.

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

6. Matriks Skalar

   Matriks yang elemen-elemen pada diagonalnya bernilai sama, sedangkan elemen lainnya bernilai nol.

2.1.3 Operasi-Operasi pada Matriks

Terdapat beberapa operasi-operasi untuk mengolah matriks diantaranya adalah:

1. Penjumlahan dan Pengurangan Matriks

   Operasi penjumlahan dan pengurangan dapat dilakukan pada dua buah matriks yang memiliki ukuran yang sama. Penjumlahan dan pengurangan matriks dapat dilakukian dengan menjumlahkan atau mengurangi elemen-elemen yang bersesuaian pada kedua matriks.

2. Perkalian Matriks dengan Matriks

   Operasi perkalian matriks dapat dilakukan pada dua buah matriks (A dan B) jika jumlah kolom matriks A = jumlah baris matriks B. Aturan perkalian.

   Misalkan A_{mn} dan B_{nk} maka $A_{mn}\ B_{nk} = C_{mk}$ dimana elemen-elemen dari C merupakan penjumlahan dari perkalian elemen-elemen A baris i dengan elemen– elemen B kolom j

3. Perkalian Matriks dengan Skalar

   Suatu matriks dapat dikalikan suatu skalar k dengan aturan tiap-tiap elemen pada A dikalikan dengan k

4. Transpose Matriks

   Transpose matriks A (dinotasikan A^t) didefinisikan sebagai matriks yang baris-barisnya merupakan kolom dari A.

Sifat-sifat dari operasi matriks:

- A+B = B+A
- A+ (B+C) = (A+B) + C
- AB ≠ BA
- A (BC) = (AB) C
- $(A^t)^t = A$
- $(AB)^t = B^t A^t$

2.1.4 Matriks Invers

Jika A dan B adalah matriks persegi, dan berlaku AB = BA = I maka dikatakan matriks A dan B saling invers. B disebut invers dari A, atau ditulis A^{-1}. Matriks yang mempunyai invers disebut *invertible*.

Untuk mencari invers matriks persegi berordo 2×2, Jika $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dengan $ad - bc \neq 0$, maka invers dari matriks A atau A^{-1} adalah sebagai berikut:

$$A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Jika $ad - bc = 0$, maka matriks tersebut tidak mempunyai invers, atau disebut matriks singular.

Sifat-sifat matriks persegi yang mempunyai invers:

- $(AB)^{-1} = B^{-1}.A^{-1}$
- $(BA)^{-1} = A^{-1}.B^{-1}$
- $(A^{-1})^t = (A^t)^{-1}$

2.2 KRIPTOGRAFI

2.2.1 Definisi dan Cara Kerja

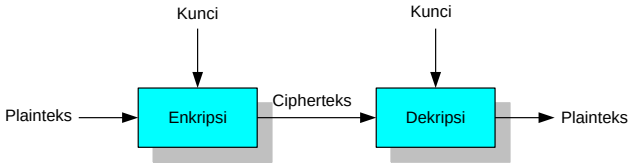
Kata *cryptography* berasal dari bahasa Yunani: krupto (*hidden* atau *secret*) dan grafh (*writing*) yang memiliki arti "*secret writing*". Kriptografi merupakan suatu ilmu untuk menjaga kerahasian dari suatu pesan dengan cara mengubahnya ke dalam suatu bentuk yang maknanya sudah tak bisa dimengerti lagi tanpa proses enkripsi.

Pesan atau *plaintext* atau *cleartext* adalah data atau informasi yang dapat dibaca dan dimengerti maknanya oleh penerima pesan. Pesan dapat berupa data atau

informasi yang dikirim (melalui kurir, saluran telekomunikasi, dan sebagainya) atau yang disimpan di dalam media perekaman (kertas, storage, dan sebagainya). Bentuk-bentuk dari pesan juga sangat beragam, diantaranya adalah teks, gambar, suara, video, tabel, atau berkas biner lainnya.

Ciphertext adalah suatu sandi dari pesan sehingga pesan tersebut tidak lagi dapat dipahami maknanya. Proses pengubahan *plaintext* menjadi *ciphertext* agar pesan tidak dapat diketahui orang lain disebut sebagai enkripsi atau *enciphering*. Sedangkan proses untuk mengembalikan *ciphertext* menjadi *plaintext* adalah dekripsi atau *deciphering*.

Kriptanalitas adalah ilmu mengubah ciphertext menjadi

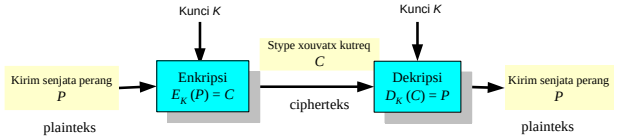


Gambar 1: Skema Enkripsi dan Dekripsi

Misalkan:
C = ciphertext
P = plaintext
Fungsi enkripsi *E* memetakan *P* ke *C*: $E(P) = C$
Fungsi dekripsi *D* memetakan *C* ke *P*: $D(C) = P$
Fungsi enkripsi dan dekripsi harus memenuhi sifat:
$D(E(P)) = P$

2.2.2 Kunci

Kunci merupakan parameter yang digunakan untuk transformasi *enciphering* dan *deciphering.*



Gambar 2: Skema Kriptografi dengan Kunci

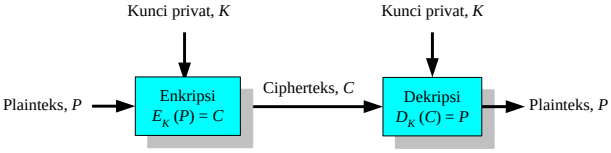
Misalkan:
C = ciphertext
P = plaintext
Fungsi enkripsi *E* memetakan *P* ke *C*: $E_K(P) = C$
Fungsi dekripsi *D* memetakan *C* ke *P*: $D_K(C) = P$
Fungsi enkripsi dan dekripsi harus memenuhi sifat:
$D_K(E_K(P)) = P$

Metode kriptografi dengan menggunakan kunci ini sendiri terdiri dari dua jenis yaitu:

1. Kriptografi kunci simetris

   Pada kriptografi kunci simetris, jumlah kunci yang digunakan hanyalah satu. Kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Karena hanya memiiki satu kunci maka kunci tersebut hanyalah *private key*.

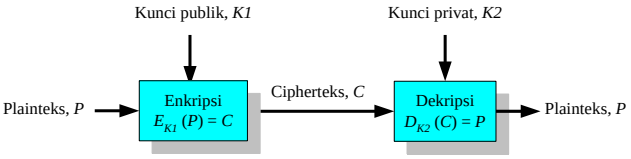
   Plaintext akan melewati proses enkripsi dan menghasilkan *ciphertext*, kemudian akan melalui proses dekripsi menggunakan kunci yang sama sehingga menjadi bentuk awalnya. Metode kunci simetris cocok digunakan dalam satu area gedung karena pengiriman pesannya tidak menggunakan penyimpanan pesan, sehingga keamanan algoritma simetris ini terletak pada keamanan pengiriman kunci dan pada panjangnya kunci yang dipergunakan. Tetapi, pada metode ini kerahasiaan kunci harus dijaga dengan sangat baik.



Gambar 3: Skema Algoritma Simetri

2. Kriptografi kunci asimetris

   Pada kunci asimetri, kunci yang digunakan untuk proses enkripsi berbeda dengan kunci yang digunakan pada proses dekripsi, berkebalikan dengan metode kunci simetris. Prinsip dasar algoritma ini adalah setiap anggota dalam jaringan kerja mempunyai 2 kunci yaitu *public key* dan *private key*. *Public key* adalah kunci yang digunakan untuk proses enkripsi. Sedangkan, *private key* adalah kunci yang digunakan untuk proses dekripsi. *Private key* hanya dimiliki oleh orang yang melakukan proses enkripsi saja dan *public* key diketahui oleh banyak orang. Algoritma kunci asimetris lebih sering disebut sebagai kunci *public/ public key*, biasanya algoritma ini digunakan dalam jaringan komunikasi yang besar dan dinamis. Karena memiliki dua kunci yang berbeda, metode ini lebih sulit untuk dipecahkan.



Gambar 4: Skema Algoritma Asimetri

2.3 HILL CIPHER

Hill Cipher merupakan contoh algoritma kriptografi kunci simetris. Algoritma *Hill Cipher* menggunakan matriks berukuran m x m yang bersifat *invertible* dalam modulo 26 sebagai kunci untuk melakukan enkripsi dan dekripsi.

Prosesnya adalah

1. Tentukan matriks *K* berordo m x m yang bersifat *invertible* dalam modulo 26 sebagai kunci.
2. Ubah pesan menjadi *plaintext* alphabet A-Z tanpa spasi
3. Konversi semua karakter alfabet menjadi angka 0-25.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 5: Konversi Hill Cipher

4. Bagilah string angka tersebut ke dalam blok-blok yang mempunyai ukuran m. Jika angka-angka tersebut

tidak dapat dibagi dengan m, maka blok terakhir diisi dengan angka acak.

5. Tulis setiap blok menjadi matriks lalu kalikan matriks *P* dengan matriks *K*.
6. Kembalikan setiap hasil perkalian menjadi alfabet, maka itulah *ciphertext*-nya.

III. Proses Enkripsi dan Dekripsi Hill Cipher dengan Pemanfaatan Matriks

3.1 *Enciphering Text*

Pertama-tama menentukan pesan apa yang akan dikirim, misalkan yang akan dikirim adalah pesan dalam bentuk teks ALJABAR GEOMETRI atau ALJABARGEOMETRI setelah menghilangkan spasinya.

Lalu memilih kunci yaitu matriks berordo 3 x 3, matriks harus *invertible* ($K.K^{-1} = I$) dalam modulo 26.

$$K = \begin{bmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{bmatrix}, K^{-1} = \begin{bmatrix} 10 & 19 & 16 \\ 4 & 23 & 7 \\ 17 & 5 & 19 \end{bmatrix}$$

$$K.K^{-1} = \begin{bmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{bmatrix} \begin{bmatrix} 10 & 19 & 16 \\ 4 & 23 & 7 \\ 17 & 5 & 19 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Setelah didapatkan matriks kuncinya, maka ubah plaintext ALJABARGEOMETRI dalam bentuk alfabet ke bentuk numerik.

P = A L J A B A R G E O M E T R I

menjadi

P = 0 11 9 0 1 0 17 6 4 14 12 4 19 17 8

String P tersebut dibagi ke dalam matriks dengan 1 buah kolom dan 3 buah baris.

Untuk A L J, $P_{1,2,3} = \begin{bmatrix} 0 \\ 11 \\ 9 \end{bmatrix}$

Untuk A B A, $P_{4,5,6} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$

Untuk R G E, $P_{7,8,9} = \begin{bmatrix} 17 \\ 6 \\ 4 \end{bmatrix}$

Untuk O M E, $P_{10,11,12} = \begin{bmatrix} 14 \\ 12 \\ 4 \end{bmatrix}$

Untuk T R I, $P_{13,14,15} = \begin{bmatrix} 19 \\ 17 \\ 8 \end{bmatrix}$

Proses selanjutnya adalah menentukan *ciphertext* dari *plaintext* tersebut melalui proses enkripsi yang memanfaatkan perkalian matriks kunci dengan matriks *plaintext*.

$$C_{1,2,3} = \begin{bmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{bmatrix} \begin{bmatrix} 0 \\ 11 \\ 9 \end{bmatrix} = \begin{bmatrix} 168 \\ 196 \\ 179 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 12 \\ 14 \\ 23 \end{bmatrix}$$

$$C_{4,5,6} = \begin{bmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 8 \\ 13 \end{bmatrix}$$

$$C_{7,8,9} = \begin{bmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{bmatrix} \begin{bmatrix} 17 \\ 6 \\ 4 \end{bmatrix} = \begin{bmatrix} 112 \\ 181 \\ 111 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 8 \\ 25 \\ 7 \end{bmatrix}$$

$$C_{10,11,12} = \begin{bmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{bmatrix} \begin{bmatrix} 14 \\ 12 \\ 4 \end{bmatrix} = \begin{bmatrix} 124 \\ 214 \\ 186 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 20 \\ 6 \\ 4 \end{bmatrix}$$

$$C_{13,14,15} = \begin{bmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{bmatrix} \begin{bmatrix} 19 \\ 17 \\ 8 \end{bmatrix} = \begin{bmatrix} 209 \\ 327 \\ 272 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 1 \\ 15 \\ 12 \end{bmatrix}$$

C = 12 14 23 3 8 13 8 25 7 20 6 4 1 15 12

Jika bentuk numeric dari C dikonversi kembali ke bentuk alfabet, menjadi

C = M O X D I N I Z H U G E B P M

Maka, didapatkan *ciphertext* dari *plaintext* ALJABARGEOMETRI adalah MOXDINIZHUGEBPM.

3.2 *Deciphering Text*

Setelah melakukan proses enkripsi, maka ciphertext harus melalui proses dekripsi agar pesan yang sebenarnya yaitu ALJABAR GEOMETRI dapat diterima dengan baik.

Pertama, cari dahulu invers dari matriks kunci dalam modulo 26.

$$K^{-1} = \begin{bmatrix} 10 & 19 & 16 \\ 4 & 23 & 7 \\ 17 & 5 & 19 \end{bmatrix}$$

Lalu, ubah *ciphertext* MOXDINIZHUGEBPM ke dalam bentuk angka.

C = 12 14 23 3 8 13 8 25 7 20 6 4 1 15 12

String C tersebut dibagi ke dalam matriks dengan 1 buah kolom dan 3 buah baris

Untuk M O X, $C_{1,2,3} = \begin{bmatrix} 12 \\ 14 \\ 23 \end{bmatrix}$

Untuk D I N, $C_{4,5,6} = \begin{bmatrix} 3 \\ 8 \\ 13 \end{bmatrix}$

Untuk I Z H, $C_{7,8,9} = \begin{bmatrix} 8 \\ 25 \\ 7 \end{bmatrix}$

Untuk U G E, $C_{10,11,12} = \begin{bmatrix} 20 \\ 6 \\ 4 \end{bmatrix}$

Untuk B P M, $C_{13,14,15} = \begin{bmatrix} 1 \\ 15 \\ 12 \end{bmatrix}$

Lalu buatlah operasi perkalian antara invers dari matriks kunci dan matriks C.

$$P_{1,2,3} = \begin{bmatrix} 10 & 19 & 16 \\ 4 & 23 & 7 \\ 17 & 5 & 19 \end{bmatrix} \begin{bmatrix} 12 \\ 14 \\ 23 \end{bmatrix} = \begin{bmatrix} 754 \\ 531 \\ 711 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 0 \\ 11 \\ 9 \end{bmatrix}$$

$$P_{4,5,6} = \begin{bmatrix} 10 & 19 & 16 \\ 4 & 23 & 7 \\ 17 & 5 & 19 \end{bmatrix} \begin{bmatrix} 3 \\ 8 \\ 13 \end{bmatrix} = \begin{bmatrix} 390 \\ 287 \\ 338 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$$P_{7,8,9} = \begin{bmatrix} 10 & 19 & 16 \\ 4 & 23 & 7 \\ 17 & 5 & 19 \end{bmatrix} \begin{bmatrix} 8 \\ 25 \\ 7 \end{bmatrix} = \begin{bmatrix} 667 \\ 656 \\ 394 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 17 \\ 6 \\ 4 \end{bmatrix}$$

$$P_{10,11,12} = \begin{bmatrix} 10 & 19 & 16 \\ 4 & 23 & 7 \\ 17 & 5 & 19 \end{bmatrix} \begin{bmatrix} 20 \\ 6 \\ 4 \end{bmatrix} = \begin{bmatrix} 378 \\ 246 \\ 446 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 14 \\ 12 \\ 4 \end{bmatrix}$$

$$P_{13,14,15} = \begin{bmatrix} 10 & 19 & 16 \\ 4 & 23 & 7 \\ 17 & 5 & 19 \end{bmatrix} \begin{bmatrix} 1 \\ 15 \\ 12 \end{bmatrix} = \begin{bmatrix} 487 \\ 433 \\ 320 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 19 \\ 17 \\ 8 \end{bmatrix}$$

Setelah didapatkan hasil perkalian, maka didapati hasil

P = 0 11 9 0 1 0 17 6 4 14 12 4 19 17 8

Lalu konversikan angka-angka tersebut ke dalam bentuk alfabet.

P = A L J A B A R G E O M E T R I

Setelah melalui proses dekripsi dari *ciphertext*, didapatkan kembali *plaintext* semula yaitu ALJABAR GEOMETRI.

Untuk melakukan serangan pada kriptografi Hill Cipher sulit karena

IV. KESIMPULAN

Algoritma Hill Cipher adalah metode kriptografi simetris karena untuk melakukan proses enkripsi dan deksripsinya hanya dibutuhkan satu buah kunci.

Dalam metode ini, untuk melakukan enkripsi dan dekripsi digunakan matriks dan aritmatika modulo.

V. UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih kepada Tuhan Yang Maha Esa, karena berkat, kasih, dan karunia-Nya penulis dapat menyelesaikan makalah ini. Penulis juga ingin berterima kasih kepada dosen mata kuliah IF2123 Aljabar Geometri, Bapak Dr. Ir. Rinaldi Munir, M.T. dan Bapak Drs. Judhi Santoso, M. Sc. karena berkat bimbingannya selama ini penulis dapat menulis makalah ini dengan sebaik-baiknya.

REFERENSI

[1] Munir, Rinaldi, *Kriptografi*, Bandung: Informatika, 2006.

[2] Stover, Christopher and Weisstein, Eric W., Matrix Inverse, diakses pada 12 Desember 2015, http://mathworld.wolfram.com/MatrixInverse.html

[3] Sibaroni,Yuliant, *Buku Ajar Aljabar Linear*, Bandung: Sekolah Tinggi Teknologi Telkom, 2002.

[4] Leon, Steven J., *Linear Algebra with Applications*, New Jersey: Pearson Prentice Hall, 2010.

[5] Zulaikha, *Invers Matriks*, diakses tangga; 12 Desember 2015, http://contohdanpenyelesaianmatrix.blogspot.co.id/2014/06/invers-matriks_5.html

[6] Salisbury University, *The Hill Cipher: A Linear Algebra Perspective*, diakses pada 12 Desember 2015, http://facultyfp.salisbury.edu/despickler/personal/Resources/LinearAlgebra/HillCipherHandoutLA.pdf

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, 15 Desember 2015

Catherine Pricilla
13514004