Penerapan Matriks dalam Kriptografi

Malvin Juanda/13514044
Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13514044@std.stei.itb.ac.id

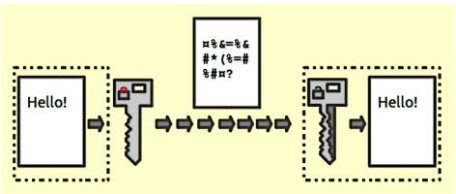
***Abstract*—Dalam era digital ini begitu banyak pertukaran informasi yang dilakukan melalui internet. Dalam proses pertukaran ini sering terjadi pencurian atau pengambilan data oleh pihak yang tidak berwenang. Bila data yang dicuri merupakan data penting, misalnya data *internet banking* maka pemilik data tersebut bisa mendapat kerugian yang cukup besar. Oleh karena itu, beberapa dekade terakhir, keamanan jaringan telah menjadi isu yang hangat di kalangan masyarakat maupun pemerintah. Berbagai metode dibuat untuk melakukan enkripsi teks, salah satunya adalah matriks. Karena matriks dapat mudah dipahami secara luas, penggunaan matriks sangat efisien dalam enkripsi teks. Sistem ini menerima teks dari pengguna kemudian menggunakan algoritma enkripsi untuk mengenkripsi sesuai dengan posisi karakter dalam matriks.**

***Keywords*—Matriks, Enkripsi, *public key*, *private key*.**

I. PENDAHULUAN

Perkembangan teknologi internet yang cepat, membuat berbagai data lebih sering disimpan dalam bentuk digital. Data digital yang telah disimpan biasanya ditransfer ke jarngan internet, dengan email maupun *cloud system*, yang kemudian dapat dilihat oleh orang tertentu. Namun, seringkali terjadi pembajakan terhadap data yang kita simpan oleh para peretas. Disinilah peran kemanan jaringan diterapkan. Salah satu teknik untuk mengamakan informasi adalah kriptografi. Dalam kriptografi, kita menyembunyikan data yang kita miliki dari pengguna yang tidak berwenang dengan menggunakan berbagai teknik yang telah dikembangkan. Enkripsi merupakan salah satu teknik dimana data yang telah kita simpan diubah ke bentuk lain sehingga hanya bisa dilihat oleh pihak berwenang.

Salah satu konsep penting dalam enkripsi yaitu private key dan public key. Private key disimpan oleh pihak berwenang dan digunakan untuk membaca informasi yang sudah dienkripsi. Public key merupakan kunci yang dibagikan ke publik dan hanya orang dengan pivate key yang bisa membacanya.



Gambar1. Proses enkripsi

Pengiriman data yang sudah di-enkripsi membuat data yang kita simpan menjadi lebih aman. Dalam makalah ini, teknik kriptografi yang akan digunakan adalah *Hill Chiper*.

II. LANDASAN TEORI

Untuk mengetahui aplikasi matriks dalam enkripsi teks, berikut akan dibahas teori dasar matriks, teori bilangan, dan kriptografi.

A. Matriks

Matriks merupakan kumpulan bilangan yang berbentuk segi empat yang terdiri dari baris dan kolom.

A_{ij} untuk setiap i = 1, 2, 3, …, m dan j = 1, 2, 3, …, n dinamakan elemen matriks yang terletak pada baris ke-i dan kolom ke-j. Sedangkan, i dan j merupakan indeks matriks.

Orde suatu matriks merupakan hasil kali jumlah baris dan jumlah kolom.

1. Jenis Matriks

Matriks memiliki banyak jenis, untuk memudahkan kita dalam memahami Enkripsi dengan kriptografi, akan dibahas beberapa saja.

- Matriks Pesergi
  Matriks pesetgi merupakan matriks yang ukuran barisnya sama dengan ukuruan kolomnya (n X n).

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

- Matriks Segitiga
  Matriks segitiga memiliki dua jenis yaitu matriks segitiga atas dan matriks segitiga bawa. Matriks segitiga atas merupakan matriks pesergi yang elemen dibawah elemen diagonal adalah nol. Sedangkan, matriks segitiga atas matriks persergi yang elemen diatas elemen diagonalnya adalah nol.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{bmatrix} \qquad \boldsymbol{B} = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 4 & 5 & 6 \end{bmatrix}$$

- Matriks Tranpose
  Matriks transpose diperoleh dari mengubah baris menjadi kolom.

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

2. Perkalian Matriks

- Perkalian matriks dengan skalar

  Perkalian matriks dengan sklar akan menghasilkna matriks dengan elemen yang sama tetapi dengan elemen setiap matriks yang dikalikan dengan bilangan sklar tersebut.

  Misalkan k ∈ Bilangan Riil $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dan maka

  $$k \times A = k \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ka & kb \\ kc & kd \end{bmatrix}$$

- Perkalian matriks dengan matriks lain

  Misalkan matriks $A_{m \times n}$ dan $B_{x \times y}$, maka

  - A×B bisa dilakukan jika n=p dan hasil ukuran matriks m × q
  - B×A bisa dilakukan jika q=m dan hasil ukuran matriks p × n

  Elemen baris ke-1 kolom ke-2 merupakan hasil penjumlahan dari hasil kali elemen pada baris ke-1 matriks A dengan elemen pada kolom ke-2 matriks B.

  Misalkan $A = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}$ dan $B = \begin{bmatrix} p & s \\ q & t \\ r & u \end{bmatrix}$ maka

  $$A \times B = \begin{bmatrix} ap + bq + cr & as + bt + cu \\ dp + eq + fr & ds + et + fu \end{bmatrix}$$

3. Operasi Baris Elementer

Operasi baris elementer atau disingkat OBE merupakan operasi aritmatika yang terjadi pada setiap elemen pada baris.

Operasi Baris Elementer meliputi :

- Pertukaran matriks
- Perkalian baris dengan konstanta tak nol
- Penjumlahan suatu baris dengan hasil perkalian baris lain dengan konstanta tak nol

Beberapa definisi yang perlu diketahui dalam OBE :

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 5 & 6 & 7 \\ 0 & 0 & 8 & 9 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

- Bilangan 1 (a_{11}) dinamakan satu utama
- Bilangan 5 (a_{22}) dinamakan unsur pertama tak nol
- Baris pertama, kedua, dan ketiga dinamakan baris tak nol karena semua elemennya tidak nol
- Baris ke-empat dinamakan baris nol

Hasil dari OBE adalah matriks (esilon baris) yang memiliki ciri-ciri sebagai berikut :

- Pada baris tak nol elemen pertamanya adalah 1 (satu utama)
- Pada baris tak nol berikutnya pembuat satu utama berada lebih kanan
- Baris nol diletakkan paling bawah

Eliminasi Gauss-Jordan menghasilkan matriks (esilon baris tereduksi) dengan elemen selain satu utama adalah nol.

Misalkan sebuah matriks $A = \begin{bmatrix} 1 & 2 & 0 \\ 3 & 2 & -1 \\ 2 & 1 & -2 \end{bmatrix}$

Untuk mencari matriks esilon baris gunakan OBE :

$$b_2 - 3b_1 \sim \begin{bmatrix} 1 & 2 & 0 \\ 0 & -4 & -1 \\ 2 & 1 & -2 \end{bmatrix}$$

$$b_2/4 \sim \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & -\frac{1}{4} \\ 2 & 1 & -2 \end{bmatrix}$$

$$b_3 - 2b_1 \sim \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & -\frac{1}{4} \\ 0 & -3 & -2 \end{bmatrix}$$

$$b_3 - 2b_1 \sim \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & -\frac{1}{4} \\ 0 & -3 & -2 \end{bmatrix}$$

$$b_3 + 3b_2 \sim \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & -\frac{1}{4} \\ 0 & 0 & -\frac{11}{4} \end{bmatrix}$$

4. Matriks Invers

Suatu matriks pesergi A dikatakan memiliki invers apabila ada matriks pesergi B sehingga

$$A.B = B.A = I$$

dengan I adalah matriks identitas dan matriks B merupakan invers dari matriks A (A^{-1}).

Cara menentukan matriks invers dari suatu matriks dapat ditentukan dengan OBE, yaitu :

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

- Lakukan OBE pada ruas kiri matriks A bersamaan dengan matriks identitas pada ruas kanan
- Lakukan sampai didapatkan matriks esilon baris tereduksi pada matriks A
- Matriks identitas pada ruas kanan sekarang menjadi matriks invers dan matriks A menjadi matriks identitas
- Jika pada OBE ditemukan baris nol pada matriks A maka matriks A tidak memiliki invers

Misalkan matriks $A = \begin{bmatrix} 2 & 2 & -1 \\ 6 & 2 & -1 \\ 0 & 1 & 1 \end{bmatrix}$

Untuk mencari matriks invers gunakan OBE dan matriks identitas :

$$\left(\begin{array}{ccc|ccc} 2 & 2 & -1 & 1 & 0 & 0 \\ 6 & 2 & -1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\left(\begin{array}{ccc|ccc} 1 & 1 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & -4 & 2 & -3 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\left(\begin{array}{ccc|ccc} 1 & 1 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & -4 & 2 & -3 & 1 & 0 \end{array}\right)$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & -\frac{3}{2} & \frac{1}{2} & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 6 & -3 & 1 & 4 \end{array}\right)$$

$$\left(\begin{array}{ccc|ccc} 1 & 1 & -\frac{3}{2} & \frac{1}{2} & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{6} & \frac{2}{3} \end{array}\right)$$

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 0 & -\frac{1}{4} & \frac{1}{4} & 0 \\ 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{6} & \frac{1}{3} \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{6} & \frac{2}{3} \end{array}\right)$$

B. Aritmatika Modulo

Operator yang digunakan pada aritmatika modulo adalah mod. Operasi aritmatika ini jika digunakan pada pembagian bulat menghasilkan sisa pembagian. Contoh:

26 mod 4 = 2

24 mod 6 = 0

Cara untuk menyatakan dua buah bilangan memiliki sisa pembagian yang sama adalah dengan *kongruen*.

$$a \equiv b \pmod{}$$

Artinya a dan b kongruen dalam modulo m. Penulisan diatas sama saja dengan:

$$a \pmod{m} = b \pmod{m}$$

Contoh:

$26 \equiv (2 \bmod 4) \Leftrightarrow 26 \pmod 4 = 2 \pmod 4$

Kekongruenan $a \equiv b \pmod{}$ dapat juga dituliskan dalam hubungan:

$$a = b + km$$

1. Teorema Fermet

Jika p adalah bilangan prima dan a adalah bilangan bulat yang habis dibagi dengan p, yitu PBB(a,p)=1, maka

$$a^{p-1} \equiv 1 \ (mod\ p)$$

2. Chinese Reminder Theorem

Misalkan m_1, m_2, m_3, …, m_n adalah bilangan bulat positif sedemikian sehingga PBB(m_i,m_j) = 1 untuk $i \neq j$. Maka sistem kongruen lanjar

$$x \equiv a_k \ (mod\ m_k)$$

Mempunyai sebuah solusi unik modulo m = m_1. m_2. …. m_n.

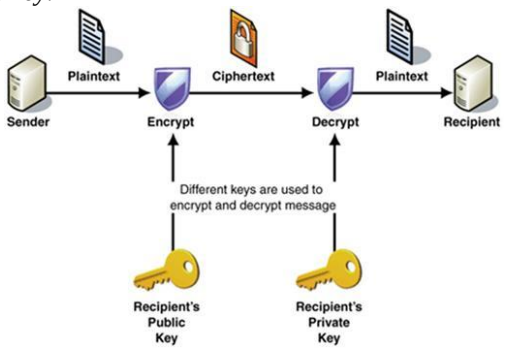
C. Kriptogafi

1. Pengertian Kriptografi

Kriptografi merupakan ilmu yang mempelajari teknik-teknik untuk mengamankan komunikasi dari pihak yang tidak berwenang.

Hal yang penting dalam kriptografi yaitu proses enkripsi dan dekripsi. Dalam proses enkrispi, pesan yang akan dikirimkan atau disebut *plaintext* akan diubah menjadi *chipertext* (pesan yang sudah diubah oleh algoritma enkripsi).

Untuk mengubah *plaintext* menjadi *chipertext* diperlukan sebuah kunci yaitu *public key*. Sedangkan, unuk mengubah *chipertext* menjadi *plaintext* diperlukan *private key*.



Gambar2. Proses kriptografi

Sumber: http://wpengine.netdna-cdn.com/

2. Hill Chiper

Hill Chiper merupakan *polygraphic substiution Chiper*. *Hill Chiper* menggunakan matematika Aljabar Linear, yaitu matriks. Selain aljabar linear, Hill chiper juga menggunakan arimatika modulo dalam proses enkripsi dan dekripsi.

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

Gambar3. Tabel konversi huruf

Proses enkripsi Hill Chiper :

- Buatlah sebuah kunci dalam bentuk matriks. Ukuran matriks 2x2 jika bekerja dengan diagraf, 3x3 jika bekerja dengan triagraf dan seterusnya
- Masukkan data yang akan dienkripsi ke dalam matriks
- Ubah data tersebut ke dalam bentuk numerik seperti Gambar2
- Kalikan data dalam matriks dengan kunci
- Lakukan modulo 26 pada hasil perkalian matriks agar mendapatkan angka yang kecil. Jika modulo 26 menghasilkan angka yang melebihi tabel konversi lakukan modulo yang menghasilkan angka yang terdapat pada tabel
- Konversi kembali numerik yang didapat ke alfabet sesuai dengan Gambar2

Proses dekripsi Hill Chiper:
- Lakukan invers pada *private key*
- Kalikan *private key* dengan hasil dekripsi
- Lakukan modulo pada matriks untuk menghasilkan angka yang tersedia di tabel konversi
- Ubah angka pada matriks menjadi huruf sesuai Gambar2.

III. PROSES KRIPTOGRAFI

Kriptografi dalam makalah ini menggunakan *Hill Chiper* dalam penyelesaiannya.

A. Proses Enkripsi

Misalnya kata yang akan dienkripsi adalah 'ALJABAR GEOMETRI', maka tahap penyelesainnya adalah :

- Ubah huruf pada kata 'ALJABAR GEOMETRI' menjadi angka sesuai Gambar3. Misalnya 'A' menghasilkan '0', 'L' menghasilkan '11', dan seterusnya

  'ALJABAR' menjadi :

0	11	9	0	1	0	7

  'GEOMETRI' menjadi :

6	4	16	12	4	19	17	8

- Hasil pada tahap 1 kemudian diubah menjadi matriks dengan ukuran yang disesuaikan. Untuk 'ALJABAR GEOMETRI' akan digunakan matriks ukuran 3×5 karena total huruf ada 15. Kemudian, isi angka tersebut kedalam matriks 3×5

0	11	9	0	1
0	7	6	4	16
12	4	19	17	8

Gambar4. Hasil konversi

- Matriks pada Gambar4 merupakan matriks triagraf maka kunci yang diperlukan merupakan matriks 3×3 atau memiliki 9 huruf. Kunci yang digunakan adalah 'BESAR HATI' dan ubah menjadi angka sesuai tahap 1 dan 2

1	4	18
0	17	7
9	19	8

Gambar5. *Private key*

- Kalikan matriks pada Gambar5 dan Gambar4

$$\begin{pmatrix}1 & 4 & 18\\0 & 17 & 7\\9 & 19 & 8\end{pmatrix}\begin{pmatrix}0 & 11 & 9 & 0 & 1\\0 & 7 & 6 & 4 & 16\\12 & 4 & 19 & 17 & 8\end{pmatrix}$$

$$=\begin{pmatrix}216 & 111 & 375 & 322 & 209\\84 & 147 & 235 & 187 & 328\\96 & 264 & 347 & 212 & 377\end{pmatrix}$$

Gambar6. Hasil perkalian *private key* dan *plain text*

Lakukan modulo 26 pada setiap elemen matriks

$$\begin{pmatrix}216 & 111 & 375 & 322 & 209\\84 & 147 & 235 & 187 & 328\\96 & 264 & 347 & 212 & 377\end{pmatrix} \pmod{26}$$

$$=\begin{pmatrix}8 & 7 & 11 & 10 & 1\\6 & 17 & 1 & 5 & 16\\18 & 4 & 9 & 4 & 13\end{pmatrix}$$

Gambar7. Hasil modulo

- Ubah angka pada matriks menjadi huruf dengan menggunakan Gambar2. Hasil enkripsi menjadi : 'IHLKAGRBFQSEJEO'

B. Proses Dekripsi

Misalnya kata yang akan didekripsi adalah 'WPSKEHKVQGKAIPR' seperti contoh diatas, maka tahap penyelesaiannya adalah:

- Kita sudah mengetahui *private key* adalah 'HANCUR HATI' dan berukuran 3×3 seperti pada Gambar5. Berarti kita dapat mengetahui ukuran matriks *plain text* yaitu 3x5.

8	7	11	10	1
6	17	1	5	16
18	4	9	4	13

Gambar8. *Plain text*

- Lakukan invers pada *private key*. Sehingga, didapatkan AB=I (mod 26). Dengan A adalah *private key*, B adalah hasil invers, dan I adalah matriks identitas.

25	18	6
5	8	11
25	3	3

Gambar9. Hasil invers

- Kasil matriks pada Gambar9 dengan *plain text* pada Gambar8

$$\begin{pmatrix}25 & 18 & 6\\5 & 8 & 11\\25 & 3 & 3\end{pmatrix}\begin{pmatrix}8 & 7 & 11 & 10 & 1\\6 & 17 & 1 & 5 & 16\\18 & 4 & 9 & 4 & 13\end{pmatrix}$$

$$=\begin{pmatrix}416 & 505 & 347 & 364 & 391\\286 & 215 & 162 & 134 & 276\\272 & 238 & 305 & 277 & 112\end{pmatrix}$$

Gambar10. Hasil perkalian

- Lakukan modulo pada setiap elemen di matriks pada Gambar10.

$$\begin{pmatrix} 416 & 505 & 347 & 364 & 391 \\ 286 & 215 & 162 & 134 & 276 \\ 272 & 238 & 305 & 277 & 112 \end{pmatrix} \pmod{26}$$

$$= \begin{pmatrix} 0 & 11 & 9 & 0 & 1 \\ 0 & 7 & 6 & 4 & 16 \\ 12 & 4 & 19 & 17 & 8 \end{pmatrix}$$

Gambar 11. Hasil dekripsi

- Ubahlah angka pada Gambar11 menjadi huruf dengan Gambar 2. Kita akan mendapatkan 'ALJABAR GEOMETRI'

V. Conclusion

Penggunaan kriptografi sangat berguna khususnya dalam *password* untuk *site*, komputer, dsb yang mengandung informasi yang penting bagi kita. Apabila *password* telah dienkripsi maka akan sangat sulit didekripsi karena mengandung banyak kemungkinan dalam pemecahannya.

Kriptografi memiliki banyak teknik dalam penyelesaiannya. Salah satu teknik kriptografi adalah penggunaan aljabar linear yaitu matriks dan aritmatika modulo. Penggunaan matriks sangat berguna karena dalam proses enkripsi diperlukan *private key* yang memiliki ukuran matriks tertentu. Jika ukuran matriks *private key* salah dalam proses dekripsi maka akan menghasilkan hasil yang salah.

VII. Acknowledgment

Pertama penulis ingin mengucapkan puji syukur kepada Tuhan karena dengan bimbingannya penulis bisa menyelesaikan makalah ini. Penulis juga mengucapkan terima kasih kepada Dr. Ir. Rinaldi Munir atas bimbingan dan jasa beliau yang selama ini telah mengajar dan memberikan Tak lupa juga penulis berterima kasih atas teman-teman seperjuangan yang telah memberikan masukan kepada penulis.

References

[1] Adiwijaya. *Aljabar Liniar Elementer*.
[2] *Hill Chiper Project*. massey.limfinity.com/207/hillcipher.pdf, diakses 15 Desember 2015.
[3] Munir, Rinaldi. "Matematika Diskrit." Informatika, Bandung: 2010.
[4] http://matrix.reshish.com/inverse.php, diakses 15 Desember 2015
[5] http://www.wolframalpha.com/widgets/view.jsp?id=2de311966212471dec23077dd840840d, diakses15 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, 12 Desember 2015

Malvin Juanda/13514044