Penerapan Matriks dalam Kriptografi *Hill Cipher*

Micky Yudi Utama/13514011
Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
micky.yu@students.itb.ac.id

Abstrak—Makalah ini akan membahas mengenai penerapan matriks dalam bidang kriptografi khususnya dalam algoritma *Hill Cipher*. *Hill Cipher* menggunakan matriks $n \times n$ sebagai kunci untuk proses enkripsi dan proses dekripsinya. Karena menggunakan matriks sebagai kunci, *Hill Cipher* menjadi sebuah algoritma dalam kriptografi yang sulit dipecahkan oleh kriptanalis jika kriptanalis tersebut hanya memiliki *ciphertext*-nya saja, namun akan dapat dengan sangat mudah dipecahkan jika kriptanalis memiliki *ciphertext* dan potongan dari *plaintext*-nya.

Kata kunci: kriptografi, matriks, *Hill Cipher*, *plaintext, ciphertext,* enkripsi, dekripsi, kriptanalis.

1. PENDAHULUAN

Salah satu hal yang paling berkembang dalam hidup manusia adalah metode dan alat yang digunakan untuk menyampaikan pesan. Dahulu penyampaian pesan dilakukan dengan tatap muka/secara langsung. Penyampaian pesan hanya bisa dilakukan jika penyampai pesan dan penerima pesan bertemu secara langsung. Seiring dengan perkembangan zaman, muncullah alat-alat yang dapat digunakan untuk menyampaikan pesan, seperti surat, telegraf, *mobile phone*, e-mail, dan lain-lain. Hingga sekarang metode dan alat penyampaian pesan masi terus berkembang. Tentu itu merupakan hal yang baik, namun di sisi lain semakin berkembangnya teknologi penyampaian pesan, semakin mudah pula pesan yang ingin disampaikan dilihat atau bahkan diganti oleh orang lain. Oleh karena itu muncullah sebuah ilmu yang dinamakan Kriptografi. Kriptografi merupakan ilmu pengetahuan sekaligus seni untuk menjaga kerahasiaan pesan yang ingin disampaikan.

Salah satu algoritma Kriptografi yang ada yaitu *Hill Cipher, Hill Cipher* menggunakan matriks n × n sebagai kunci untuk proses enkripsi dan proses dekripsinya. Dasar teori matriks yang digunakan dalam *Hill Cipher* antara lain adalah perkalian matriks dan invers matriks.

2. KRIPTOGRAFI

2.1 Pengertian Kriptografi

Kata kriptografi pertama kali berasal dari bahasa Yunani yaitu ”kryptos" yang artinya tersembunyi, dan "graphein" yang artinya tulisan. Awalnya kriptografi dianggap sebagai suatu ilmu untuk menyembunyikan/menjaga pesan, tetapi seiring dengan perkembangan zaman pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi. Kriptografi menurut KBBI yaitu suatu teknik yang mengubah data menjadi berbeda dari aslinya dengan menggunakan algoritma matematika sehingga orang yang tidak mengetahui kuncinya tidak akan dapat membongkar data tersebut.

2.2 Sejarah Kriptografi

Kegiatan penulisan pesan rahasia yang tertua dapat ditemukan pada peradaban Mesir Kuno, yakni pada tahun 3000 SM. Bangsa Mesir Kuno menggunakan ukiran rahasia yang disebut dengan *hieroglyphics* untuk menyampaikan pesan rahasia kepada orang lain.

Gambar 2.2.1 *Hieroglyphics* (www.123rf.com)

Kemudian pada tahun 1900 SM, digunakan teknik transformasi kriptografi di "tomb inscription".

Kemudian kegiatan penggunaan kriptografi selanjutnya ditemukan pada tahun 400 SM, Sparta di Yunani memanfaatkan kriptografi di bidang militer dengan menggunakan alat yang dinamakan *scytale*. *Scytale* merupakan pita panjang dengan bahan daun papyrus yang dibaca dengan cara digulungkan ke sebatang silinder.

Gambar 2.2.2 *Scytale*
(http://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html)

Pada abad 9 M, seorang ilmuwan Islam bernama Abu Yusuf Ya'qub ibn 'Ishaq as-Shabbah al Kindi atau dikenal dengan Al-Kindi menemukan teknik kriptanalis. Ia juga menuliskan kitab tentang seni memecahkan kode yang berjudul Risalah fi Istikhraj al-Mu'amma (manuskrip untuk memecahkan pesan-pesan Kriptografi). Terinsipirasi dari perulangan huruf dalma Al-Qur'an, Al-Kindi menemukan teknik analisis frekuensi, yaitu sebuah teknik untuk memecahkan *ciphertext* berdasarkan frekuensi kemunculan karakter pada sebuah pesan.

Kriptografi berkembang secara pesat dari zaman ke zaman. Perkembangan tersebut dapat dilihat dari segi kekuatan rahasia pesan, metode yang digunakan untuk enkripsi dan dekripsi, dan lain-lain. Sampai sekarang sudah banyak algoritma Kriptografi, seperti *Data Encryption Standard (*DES), *International Data Encryption Algorithm* (IDEA), *Digital Signature Algorithm* (DSA).

2.3 Prinsip Kerja Kriptografi

Terdapat dua fungsi-fungsi yang mendasar dalam kriptografi, yaitu fungsi enkripsi dan fungsi dekripsi.

Fungsi enkripsi yaitu fungsi untuk mengubah suatu pesan asli (*plaintext*) menjadi suatu pesan sandi (*ciphertext*). Fungsi enkripsi dapat dituliskan sebagai berikut:

C = E (P)

dimana

C = pesan sandi (*ciphertext*)
E = fungsi enkripsi
P = pesan asli (*plaintext*)

Fungsi dekripsi yaitu fungsi untuk mengubah suatu pesan sandi (*ciphertext*) kembali menjadi pesan asli (*plaintext*). Fungsi dekripsi dapat dituliskan sebagai berikut:

P = D (C)

dimana

P = pesan asli (*plaintext*)
D = fungsi dekripsi
P = pesan sandi (*ciphertext*)

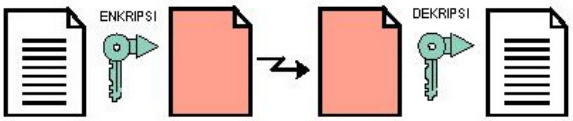
Fungsi enkripsi dan fungsi dekripsi sering diberi parameter tambahan yang disebut sebagai kunci (*key*).

2.4 Jenis-Jenis Kriptografi

Jenis kriptografi berdasarkan kunci:

1. Algoritma Simetris

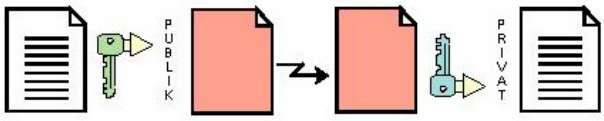
Algoritma simetris merupakan algoritma dimana kunci yang digunakan dalam proses enkripsi dan proses dekripsi sama. Kunci dalam algoritma ini bersifat rahasia (*public key*) sehingga algoritma ini sering disebut algoritma kunci rahasia. Contoh algoritma yang menggunakan kunci simetris: *Data Encryption Standard* (DES), RC2, RC4, RC5, RC6, *International Data Encryption Algorithm* (IDEA), *Advanced Encryption Standard* (AES), *On Time Pad* (OTP), A5, dan lain sebagainya.



Gambar 2.4.1 Kunci Simetris
(lovelyirmaonline.wordpress.com)

2. Algoritma Asimetris

Algoritma asimetris merupakan algoritma dimana kunci yang digunakan dalam proses enkripsi dan proses dekripsi berbeda. Kunci yang digunakan dalam proses enkripsi adalah kunci publik (*public key*) sehingga algoritma ini sering disebut algoritma kunci publik. Sedangkan kunci yang digunakan untuk proses dekripsi adalah kunci rahasia (*private key*). Contoh algoritma yang menggunakan kunci asimetris: *Digital Signature Algorithm* (DSA), RSA, *Diffle-Hellman* (DH), *Elliptic Curve Cryptography* (ECC), Kriptografi Quantum, dan lain sebagainya.



Gambar 2.4.2 Kunci Asimetris
(lovelyirmaonline.wordpress.com)

2.5 Teknik-Teknik Kriptanalis

Kriptanalisis adalah ilmu dan seni untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci dari algoritma yang digunakan. Orang yang melakukan kriptanalisis disebut kriptanalis. Ada banyak teknik-teknik yang sudah ditemukan oleh para kriptanalis.

Berikut merupakan beberapa teknik yang paling umum untuk digunakan:

1. *Known-Plaintext Analysis* merupakan teknik kriptanalis yang digunakan jika kriptanalis mengetahui *ciphertext* dan potongan dari *plaintext*.

2. *Chosen-Plaintext Analysis* merupakan teknik kriptanalis yang membandingkan dan menganalisa contoh *plaintext* dan *ciphertext*-nya. Dalam teknik ini, kriptanalis bebas untuk menentukan *plaintext* yang diinginkannya.

3. *Ciphertext-Only Analysis* merupakan teknik kriptanalis yang digunakan jika kriptanalis hanya mengetahui *cipertext*-nya saja. Teknik kriptanalis ini membutuhkan akurasi yang sangat tinggi.

Selain tiga teknik di atas, banyak lagi teknik-teknik yang digunakan kriptanalis seperti *Man-in-the-middle attack, Timing/differential power analysis, Corelation, Rubber-hose cryptanalysis*.

3. *HILL CIPHER*

Hill Cipher diciptakan oleh Lester S. Hill pada tahun 1929. *Hill Cipher* menggunakan matriks persegi sebagai dasar dalam melakukan proses enkripsi dan proses dekripsi, algoritma ini dibuat dengan tujuan untuk menciptakan kode yang tidak dapat dipecahkan dengan teknik analisis frekuensi.

Hill Cipher tidak mengganti elemen pada *plaintext* dengan elemen lainnya yang sama pada *ciphertext*. *Hill Cipher* merupakan *polyalphabetic cipher* yang dapat dikategorikan sebagai *block cipher* karena *plaintext* yang akan diproses terlebih dahulu dibagi menjadi beberapa block tertentu. Setiap elemen dalam satu blok akan mempengaruhi elemen lainnya di blok tersebut dalam proses enkripsi dan proses dekripsinya sehingga elemen yang sama belum tentu akan berubah menjadi elemen yang sama pula.

Hal tersebutlah yang membuat *Hill Cipher* menjadi suatu algoritma yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui *chipertext*-nya saja. Namun, jika sang kriptanalis memiliki *ciphertext* serta potongan *plaintext* maka algoritma ini dapat dengan sangat mudah dipecahkan. Teknik kriptanalis ini disebut *known-plaintext attack.*

Dasar dari *Hill Cipher* adalah aritmatika modulo terhadap matriks. *Hill Cipher* menggunakan perkalian matriks dan invers matriks dalam penerapannya. Kunci pada *Hill Cipher* merupakan matriks n × n dengan n merupakan ukuran blok. Matriks yang menjadi kunci harus merupakan matriks yang *invertible*, yaitu matriks yang memiliki invers. Hal tersebut dikarenakan invers dari matriks tersebutlah yang menjadi kunci dalam melakukan proses dekripsi.

3.1 Teknik Enkripsi *Hill Cipher*

Proses enkripsi pada *Hill Cipher* dilakukan per blok *plaintext*. Ukuran blok sama dengan ukuran matriks kunci yang dipilih. Sebelum membagi teks menjadi deretan blok-blok, plaintext terlebih dahulu dikonversi menjadi angka. Pengkonversian dilakukan dengan aturan A = 1, B = 2, C = 3, hingga Y = 25. Karakter Z diubah menjadi 0.

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

Gambar 3.1.1 Konversi Alfabet ke Angka dalam *Hill Cipher* (https://muamalkhoerudin.wordpress.com/2015/03/22/algoritma-hill-cipher-sandi-hill/)

Tahap-tahap dalam melakukan enkripsi *Hill Cipher:*

Misalkan *plaintext* yang akan dienkripsi adalah:

P = ILOVEALJABARGEOMETRI

1. Melakukan konversi dari alfabet ke angka terhadap *plaintext*. Hasil dari konversi *plaintext* P:

   P = 9 12 15 22 5 1 12 10 1 2 1 18 7 5 15 13 5 20 18 9

2. Memilih sebuah kunci matriks n × n yang *invertible* secara acak, dalam hal ini diambil:

$$K = \begin{matrix} 3 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 2 \end{matrix}$$

3. Membagi *plaintext* menjadi beberapa blok sesuai dengan ukuran matriks kunci. Dalam hal ini, karena matriks kunci K berukuran 3 × 3, maka *plaintext* dibagi menjadi blok yang masing-masing bloknya berukuran 3 karakter. Karena pada blok terakhir hanya terdapat 2 karakter, maka diberi tambahan 1 karakter berdasarkan karakter terakhir. Dalam hal ini karakter yang ditambahkan yaitu I. Berikut merupakan blok pertama dari *plaintext* P:

$$B1 = \begin{matrix} 9 \\ 12 \\ 15 \end{matrix}$$

4. Melakukan enkripsi pada blok *plaintext* dengan melakukan perkalian antara matriks kunci K dengan matriks blok B. Berikut hasil enkripsi dari blok pertama:

$$E1 = \begin{matrix} 3 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 2 \end{matrix} \times \begin{matrix} 9 \\ 12 \\ 15 \end{matrix} = \begin{matrix} 39 \\ 36 \\ 42 \end{matrix}$$

5. Matriks hasil enkripsi kemudian di modulo 26 agar angka dari matriks tersebut dapat berkorespondensi

dengan huruf-huruf yang ada. Berikut hasil modulo dari enkripsi blok pertama:

$$E1 \; mod \; 26 = \begin{matrix} 13 \\ 10 \\ 16 \end{matrix}$$

6. Mengulangi langkah 4 dan 5 sampai semua blok matriks berhasil terenkripsi. Berikut merupakan hasil enkripsi semua blok:

   E = 13 10 16 19 2 7 20 23 12 7 21 11 0 1 9 18 12 19 11 10 1

7. Mengkonversi hasil enkripsi menjadi alfabet. Berikut hasil konversi dari E:

   C = MJPSBGTWLGUKZAIRLSKJA

Dapat dilihat bahwa hasil enkripsi dengan metode *Hill Chiper* memiliki pola yang tidak mirip dengan *plaintext*-nya. Hal inilah yang menyebabkan *Hill Cipher* menjadi algoritma yang sangat sulit untuk dipecahkan oleh kriptanalis jika hanya diketahui *ciphertext*-nya saja.

3.2 Teknik Dekripsi *Hill Cipher*

Proses dekripsi *Hill Cipher* pada dasarnya memiliki metode yang sama dengan proses enkripsi *Hill Cipher*. Hanya saja kunci yang digunakan merupakan invers dari kunci yang digunakan dalam proses enkripsi.

Tahap-tahap dalam melakukan dekripsi *Hill Cipher:*

Misalkan *ciphertext* yang akan didekripsi adalah:

C = MJPSBGTWLGUKZAIRLSKJA

Dan kunci yang digunakan untuk dekripsi adalah:

$$K^{-1} = \begin{matrix} 1 & -2 & 1 \\ -2 & 6 & -3 \\ 1 & -3 & 2 \end{matrix}$$

1. Melakukan konversi dari alfabet ke angka terhadap *ciphertext*. Hasil dari konversi *ciphertext* C:

   C = 13 10 16 19 2 7 20 23 12 7 21 11 0 1 9 18 12 19 11 10 1

2. Membagi *plaintext* menjadi beberapa blok sesuai dengan ukuran matriks kunci. Dalam hal ini, karena matriks kunci K berukuran 3 × 3, maka *ciphertext* dibagi menjadi blok yang masing-masing bloknya berukuran 3 karakter. Berikut merupakan blok pertama dari *ciphertext* C:

$$B1 = \begin{matrix} 13 \\ 10 \\ 16 \end{matrix}$$

3. Melakukan dekripsi pada blok *ciphertext* dengan melakukan perkalian antara matriks kunci dengan matriks blok B. Berikut hasil dekripsi dari blok pertama:

$$D1 = \begin{matrix} 1 & -2 & 1 \\ -2 & 6 & -3 \\ 1 & -3 & 2 \end{matrix} \times \begin{matrix} 13 \\ 10 \\ 16 \end{matrix} = \begin{matrix} 9 \\ -14 \\ 15 \end{matrix}$$

4. Matriks hasil edekripsi kemudian di modulo 26 agar angka dari matriks tersebut dapat berkorespondensi dengan huruf-huruf yang ada. Berikut hasil modulo dari enkripsi blok pertama:

$$D1 \; mod \; 26 = \begin{matrix} 9 \\ 12 \\ 15 \end{matrix}$$

5. Mengulangi langkah 3 dan 4 sampai semua blok matriks berhasil terenkripsi. Berikut merupakan hasil dekripsi semua blok:

   D = 9 12 15 22 5 1 12 10 1 2 1 18 7 5 15 13 5 20 18 9 9

6. Mengkonversi hasil dekripsi menjadi alfabet. Berikut hasil konversi dari D:

   D = ILOVEALJABARGEOMETRII

4. KESIMPULAN

Kriptografi merupakan ilmu pengetahuan sekaligus seni yang digunakan untuk menjaga kerahasiaan pesan. Salah satu algoritma dalam kriptografi yaitu *Hill Cipher*. *Hill Cipher* merupakan jenis algoritma dalam kriptografi yang tergolong kuat karena hasil enkripsi dengan *Hill Cipher* sangat sulit dipecahkan jika kriptanalis hanya memiliki *ciphertext*-nya saja

REFERENSI

[1] http://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html diakses pada tanggal 15 Desember 2015

[2] http://kriptografi-bsi.blogspot.co.id/2013/05/sejarah-singkat-perkembangan-kriptografi.html diakses pada tanggal 15 Desember 2015

[3] http://gilang-kurniawan.blogspot.co.id/2012/05/kriptografi-2-macam-macam-algoritma.html diakses pada tanggal 15 Desember 2015

[4] http://gilang-kurniawan.blogspot.co.id/2012/05/mengenal-kriptografi.html diakses pada tanggal 15 Desember 2015

[5] http://www.pelita-informatika.com/berkas/jurnal/4221.pdf diakses pada tanggal 15 Desember 2015

[6] https://muamalkhoerudin.wordpress.com/2015/03/22/algoritma-hill-cipher-sandi-hill/ diakses pada tanggal 25 Desember 2015

[7] https://matrixcalc.org/ diakses pada tanggal 16 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, 15 Desember 2015

Micky Yudi Utama/13514011