Teknik Kriptografi Hill Cipher Menggunakan Matriks

Adam Rotal Yuliandaru - 13514091
Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
adamrotal@students.itb.ac.id

***Abstrak*—Matriks adalah sebuah struktur data yang lazim digunakan dalam operasi matematika. Salah satu dari implementasi matriks adalah dalam bidang keamanan atau yang biasa disebut kriptografi. Salah satu metode kriptografi yang memanfaatkan matriks adalah kriptografi Hill Cipher.**

Hill Cipher merupakan salah satu algoritma kriptografi kunci simetriks. Algoritma Hill Cipher menggunakan matriks *invertible* berukuran n x n sebagai kunci untuk melakukan enkripsi dan dekripsi pada *chipertext.* Ide yang digunakan adalah dengan perkalian antar matriks dan melakukan invers pada matriks pada *palintext.* Karena menggunakan matriks sebagai kunci menyebabkan Hill Cipher sangat sulit dipecahkan.

Makalah ini membahas mengenai dasar mengenai dasar teori Hill Cipher termasuk didalamnya contoh enkripsi dan dekripsi Hill Cipher menggunakan matriks.

***Kata kunci* — Matriks, Hill Ciper, Kriptografi, *plaintext, chipertext, invertible*.**

I. PENDAHULUAN

Seiring dengan perkembangan jaman dan kemajuan teknologi yang sangat pesat, kerahasiaan tentang suatu data menjadi semakin penting di era sekarang. Penyampaian data dari pihak satu ke pihak lain terancam di curi informasinya oleh para *hacker* yang mencari keuntungan pribadi. Oleh karena itu mulai bermunculan metode-metode kriptografi untuk mengamankan data dari serangan *hacker*. Kriptografi merupakan ilmu atau seni untuk menjada keamanan suatu data.

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. Unuk menyelesaikan hal ini maka pesan haruslah disandikan (*encoding*). Tujuan embuat *encoding* adalah agar aman dari para pembongkar sandi sehingga hanya penerima saja yang mengetahui isinya.

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

Hill Cipher merupakan salah satu metode kriptografi kunci simetris yang memanfaatkan matriks n x n sebagai kunci. Ide dasar dari Hill Cipher adalah manipulasi kata menggunakan operasi matriks berupa perkalian dan invers.

II. MATRIKS

Matriks adalah susunan scalar elemen-elemen dalam bentuk baris dan kolom. Matriks A yang berukuran m baris dan n kolom (m x n) disimbolkan dalam bentuk:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

a_{mn}untuk setiap i = 1, 2, …, m dan j = 1, 2, …, n dinamakan unsure/entri/elemen matriks yang terletak pada baris ke-i dan kolom ke-j. Ukuran (orde) suatu matriks merupakan jumlah baris kali jumlah kolom. Jadi matriks A diatas berukuran $m\,x\,n$. Jika semua unsure matriks bernilai nol maka matriks tersebut dinamakan matriks nol. Misalkan matriks A dan B adalah matriks berukuran sama, dapat dikatan bahwa A = B, jika unsur0unsur matriks yang seletak pada kedua matriks tersebut adalah sama. [1]

2.1 Operasi Aritmatika pada Matriks

Operasi aritmatika yang biasa dilakukan terhadap matriks adalah operasi penjumlahan dan perkalian dua buad matriks, serta perkalian matriks dengan sebuah skalara.

1. Penjumlahan matriks.
   Dua buah matriks dapat dijumlahkan jika ukuran keduanya sama. Penjumlahan dilakukan dengan menambahkan setiap elemen matriks yang memiliki posisi sama.
   $$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$
2. Perkalian matriks.
   a. Perkalian suatu matriks dengan skalar.
      Suatu matriks yang dikalikan dengan skalar akan menghasilkan matriks dengan ukuran yang sama tetapi setiap unsure pada matriks dikalikan dengan skalar tersebut.

Misalkan k adalah sebuah skalar dan $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ maka

$$k\ x\ A = k \begin{pmatrix} a & b \\ b & c \end{pmatrix} = \begin{pmatrix} ka & kb \\ kb & kc \end{pmatrix}$$

b. Perkalian dua buah matriks.
Misalkan matriks A_{mxn} dan B_{pxq} maka :

- A x B bisa dilakukan jika n = p dan hasilnya berukuran m x q.
- B x a bisa dilakukan jika q = m dan hasilnya berukuran p x n.

$$A = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix}_{2x3} \quad B = \begin{pmatrix} p & s \\ q & t \\ r & u \end{pmatrix}_{3x2}$$

maka

$$A\ x\ B = \begin{pmatrix} ap + bq + cr & as + bt + cu \\ dp + eq + fr & ds + et + fu \end{pmatrix}_{2x2}$$

3. Invers Matriks
Misalkan A dan B adalah matriks bujur sangkar yang berukuran sama dan I adalah matriks identitas. Jika A . B = I maka B dinamakan invers dari matriks A (sebaliknya, A merupakan invers dari matriks B). Notasi bahwa B merupakan matriks invers dari A adalah B = A^{-1}, dan sebaliknya A = B^{-1}.

III. KRIPTOGRAFI

Kriptografi berasal dari bahasa Yunani: "*cryptos"* yang memiliki arti rahasia, sedangkan "*grapheini"* artinya tulisan. Jadi, secara morfologi kriptografi berarti tulisan yang rahasia.

Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literature, Definisi yang kita pakai dalam makalah ini: Kriptografi adalah ilmu dan seni untuk menjadga keamanan pesan [1]. Kata "seni" dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptograf, setiap orang mungkin mempunyai cara yang untuk untuk merahasiakan pesan Pada perkembangannya, kriptografi berkembang menjadi sebuah disiplin ilmu tersendiri karena teknik-teknik kriptografi dapat diformulasikan secara matematis sehingga menjadi sebuah metode yang formal.

A. Prinsip Kerja Kriptografi

Kriptografi dapat ditulis secara matematis. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi.

Enkripsi adalah proses mengubah suatu pesan asli (*plaintext*) menjadi suatu pesan dalam bahasa sandi (*ciphertext*).

$$C = E\ (M) \qquad (2.1)$$

M = pesan asli (*plaintext*).
E = proses enkripsi.
C = pesan dalam bahasa sandi (*ciphertext*).

Dekripsi adalah proses mengubah pesan asli dalam suatu bahasa sandi menjadi pesan asli kembali sehingga dapat dibaca dan dimengerti.

$$M = D\ (C) \qquad (2.2)$$

M = pesan asli (*plaintext*).
D = proses dekripsi.
C = pesan dalam bahasa sandi (*ciphertext*).

Umumnya , selain menggunakan fungsi tertentu dalam melakukan enkripsi dan dekripsi, seringkali fungsi itu diberi parameter tambahan yang disebut dengan istilah kunci.

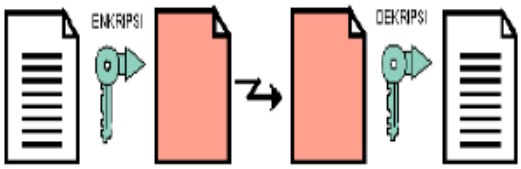
B. Jenis-jenis kunci

Jenis kunci dalam kriptografi dpaat dibagi menjadi dua, yaitu kunci simetris dan kunci asimetris.

1. Kunci Simetris

Kunci simetris adalah jenis kriptografi yang paling umum digunakan. Kunci pada proses enkripsi sama dengan pada proses dekripsi. Jadi pembuat pesan dan penerimanya harus memiliki kunci yang sama.

Siapapun yang memiliki kunci tersebut, termasuk pihak-pihak yang tidak diinginkan, dapat membuat dan membongkar rahasia *ciphertext.* Masalah yang paling jelas bukanlah masalah pengiriman *ciphertext*, melainkan masalah bagaimana menyampaikan kunci simetris tersebut kepada pihak yang diinginkan.

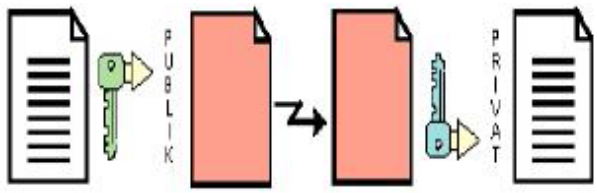


Gambar 2.0.1Kunci Simetris

2. Kunci Asimetris

Pada tahun 70-an, Whitfield Diffie dan Martin Hellman menemukan teknik enkripsi asimetris yang merevolusi dunia kriptografi, Kunci asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lainnya digunakan untuk dekripsi.

Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memilliki rahasia tertentu, dalam hal ini kunci privat, untuk membongkar sandi yang dikirim kepadanya.



Gambar 2.22Kunci Asimetris

Teknik enkripsi asimetris ini jauh lebih lambat ketimbang enkripsi dengan kunci simetris. Oleh karena itu, biasanya bukan pesan yang disandikan dengan kunci asimetris, namun hanya kunci simetrislah yang disandikan dengan kunci asimetris. Sedangkan pesannya diskirim setelah disandikan dengan kunci simetris.

C. Jenis-jenis Serangan

Selain dari pihak uang ingin menjaga agat pesan tetap aman, ada pula pihak-pihak yang ingin mengetahui pesan rahasia tersebut secara ilegal. Bahkan ada pihak yang ingin agar dapat mengubah isi pesan tersebut. Ilmu untuk mendapatkan pesan yang asli dari pesan yang telah disandikan tanpa memiliki kunci untuk membuka pesan rahasia tersebut disebut kriptanalisis. Sedangkan usaha untuk membongkar suatu pesan sandi tanpa mendapatkan kunci dengan cara yang sah dikenal dengan istilah serangan (*attack*).

Beberapa macam penyerangan terhadap pesan yang sudah dienkripsi antara lain:

1. *Ciohertext only attack*, penyerang hanya mendapatkan pesan yang sudah disandikan saja.
2. *Known plaintext attack*, penyerang mendapatkan sandi dan juga mendapat pesan asli. Disebut pula *clear-text attack.*
3. *Choosen plaintext attack*, sama dengan *known plaintext attack*, namun penyerang bahkan dapat memilih penggalan mana dari pesan asli yang disandikan.

IV. HILL CIIPHER

Hill cipher diciptakan oleh Lester S. Hill pada tahun1929. Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi [2]. Hill Cipher tidak mengganti setiap ajad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.

Hill cipher merupakan *polyalphabetic cipher* dapat dikategorikan sebagai *block cipher* karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula.

A. Dasar Teknik Hill Cipher

Dasar teknik Hill Cipher adalah aritmatika modulo terrhadap matriks. Dalam penerapannya, Hill Cipher menggunakan teknik perkalian matriks dan invers terhadap matriks.

Matriks yang digunakan pada Hill Cipher adalah matriks yang *invertible*. Matriks *invertible* adalah matriks berukuran n x n dan memiliki determinan $\neq 0$ sehingga memiliki invers. Jika matriks kunci memiliki determinan = 26, maka matriks dapat digunakan dalam proses enkripsi, namun akaan gagal ketika proses dekripsi. Sehingga penting untuk diperhatikan dalam memilih matriks kunci yang sesuai.

Sebelum membagi teks menjadi deretan blok-blok, pesan terlebih dahulu dikonversi menjadi angka-angka unik natara 0 hingga 25.

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

Tabel 4.1 Konversi Alfabet ke Angka

B. Hill Cipher Matriks

1. Enkripsi

Secara matematis, proses enkripsi pada Hill Cipher adalah:

$$C = K \,.\, P \qquad (4.1)\ [4]$$

C = *Ciphertext.*
K = Kunci.
P = *Plaintext.*

Misalkan terdapat *plaintext* P = HELLO WORLD, dan kunci $K = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$, maka:

a. Bagi *plaintext* P menjadi matriks 2 x 1 dan konversi menjadi angka sesuai table 4.1.

$$\begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} L \\ L \end{pmatrix} = \begin{pmatrix} 11 \\ 11 \end{pmatrix}$$

$$\begin{pmatrix} O \\ W \end{pmatrix} = \begin{pmatrix} 14 \\ 22 \end{pmatrix}$$

$$\begin{pmatrix} O \\ R \end{pmatrix} = \begin{pmatrix} 14 \\ 17 \end{pmatrix}$$

$$\begin{pmatrix} L \\ D \end{pmatrix} = \begin{pmatrix} 11 \\ 3 \end{pmatrix}$$

b. Kalikan setiap angka dengan matriks kunci

$K = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$.

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 14+4 \\ 21+16 \end{pmatrix} = \begin{pmatrix} 18 \\ 37 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 11 \end{pmatrix} = \begin{pmatrix} 22+11 \\ 33+44 \end{pmatrix} = \begin{pmatrix} 33 \\ 77 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 14 \\ 22 \end{pmatrix} = \begin{pmatrix} 28+22 \\ 42+88 \end{pmatrix} = \begin{pmatrix} 50 \\ 130 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 14 \\ 17 \end{pmatrix} = \begin{pmatrix} 28+17 \\ 42+68 \end{pmatrix} = \begin{pmatrix} 45 \\ 110 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 3 \end{pmatrix} = \begin{pmatrix} 22+3 \\ 33+12 \end{pmatrix} = \begin{pmatrix} 25 \\ 45 \end{pmatrix}$$

c. Lakukan operasi Mod 26 kepada setiap matriks angka tersebut agar dapat dikonversi menggunakan tabel 4.1.

$$\begin{pmatrix} 18 \\ 37 \end{pmatrix} Mod\ 26 = \begin{pmatrix} 18 \\ 11 \end{pmatrix}$$

$$\begin{pmatrix} 33 \\ 77 \end{pmatrix} Mod\ 26 = \begin{pmatrix} 7 \\ 25 \end{pmatrix}$$

$$\begin{pmatrix} 50 \\ 130 \end{pmatrix} Mod\ 26 = \begin{pmatrix} 24 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 45 \\ 110 \end{pmatrix} Mod\ 26 = \begin{pmatrix} 19 \\ 6 \end{pmatrix}$$

$$\begin{pmatrix} 25 \\ 45 \end{pmatrix} Mod\ 26 = \begin{pmatrix} 25 \\ 19 \end{pmatrix}$$

d. Ubah setiap matriks angka menjadi huruf dengan aturan konversi seperti tabel 4.1.

$$\begin{pmatrix} 18 \\ 11 \end{pmatrix} = \begin{pmatrix} S \\ L \end{pmatrix}$$

$$\begin{pmatrix} 7 \\ 25 \end{pmatrix} = \begin{pmatrix} H \\ Z \end{pmatrix}$$

$$\begin{pmatrix} 24 \\ 0 \end{pmatrix} = \begin{pmatrix} Y \\ A \end{pmatrix}$$

$$\begin{pmatrix} 19 \\ 6 \end{pmatrix} = \begin{pmatrix} T \\ G \end{pmatrix}$$

$$\begin{pmatrix} 25 \\ 19 \end{pmatrix} = \begin{pmatrix} Z \\ T \end{pmatrix}$$

e. Didapatkan pesan HELLO WORLD yang telah dienkripsi menjadi SLHYATGZT.

2. Dekripsi

Proses dekripsi pada Hill Cipher pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (invers) terlebih dahulu. Secara matematis proses dekripsi pada Hill Cipher dapat diturunkan dari persamaan 4.1.

$$C = K \,.\, P$$
$$K^{-1}.\, C = K^{-1}.\, K \,.\, P$$
$$K^{-1}.\, C = I \,.\, P$$
$$P = K^{-1}.\, C$$

Sehingga proses dekripsi dapat ditulis dengan persamaan:

$$P = K^{-1}.\, C \qquad (4.2)\ [4]$$

P = *plaintext.*
K^{-1} = invers matriks kunci.
C = *ciphertext*.

Dengan menggunakan kunci $K = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$, maka proses dekripsi diawali dengan mencari invers matriks K. Invers matriks dapat dicari menggunakan Operasi Baris Elementer (OBE) ataupun menggunakan prinsip determinan.[2]

$$K^{-1} = \begin{pmatrix} 4 & -1 \\ -3 & 2 \end{pmatrix}$$
$$K^{-1} = \begin{pmatrix} 84 & -21 \\ -63 & 42 \end{pmatrix} Mod\ 26$$
$$K^{-1} = \begin{pmatrix} 6 & 5 \\ 15 & 16 \end{pmatrix}$$

Matriks K^{-1} akan menjadi matriks kunci pada proses dekripsi, maka:

a. Bagi *plaintext* P menjadi matriks 2 x 1 dan konversi menjadi angka sesuai table 4.1

$$\begin{pmatrix} S \\ L \end{pmatrix} = \begin{pmatrix} 18 \\ 11 \end{pmatrix}$$

$$\begin{pmatrix} H \\ Z \end{pmatrix} = \begin{pmatrix} 7 \\ 25 \end{pmatrix}$$

$$\begin{pmatrix} Y \\ A \end{pmatrix} = \begin{pmatrix} 24 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} T \\ G \end{pmatrix} = \begin{pmatrix} 19 \\ 6 \end{pmatrix}$$

$$\begin{pmatrix} Z \\ T \end{pmatrix} = \begin{pmatrix} 25 \\ 19 \end{pmatrix}$$

b. Kalikan setiap angka dengan matriks kunci $K^{-1} = \begin{pmatrix} 6 & 5 \\ 15 & 16 \end{pmatrix}$.

$$\begin{pmatrix} 6 & 5 \\ 15 & 16 \end{pmatrix} \cdot \begin{pmatrix} 18 \\ 11 \end{pmatrix} = \begin{pmatrix} 108+55 \\ 270+176 \end{pmatrix} = \begin{pmatrix} 163 \\ 446 \end{pmatrix}$$

$$\begin{pmatrix} 6 & 5 \\ 15 & 16 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 25 \end{pmatrix} = \begin{pmatrix} 42+125 \\ 105+400 \end{pmatrix} = \begin{pmatrix} 167 \\ 505 \end{pmatrix}$$

$$\begin{pmatrix} 6 & 5 \\ 15 & 16 \end{pmatrix} \cdot \begin{pmatrix} 24 \\ 0 \end{pmatrix} = \begin{pmatrix} 114+0 \\ 360+0 \end{pmatrix} = \begin{pmatrix} 114 \\ 360 \end{pmatrix}$$

$$\begin{pmatrix}6 & 5\\15 & 16\end{pmatrix}.\begin{pmatrix}19\\6\end{pmatrix} = \begin{pmatrix}114+30\\285+96\end{pmatrix} = \begin{pmatrix}114\\381\end{pmatrix}$$

$$\begin{pmatrix}6 & 5\\15 & 16\end{pmatrix}.\begin{pmatrix}25\\19\end{pmatrix} = \begin{pmatrix}150+95\\375+304\end{pmatrix} = \begin{pmatrix}245\\679\end{pmatrix}$$

c. Lakukan operasi Mod 26 kepada setiap matriks angka tersebut agar dapat dikonversi menggunakan tabel 4.1.

$$\begin{pmatrix}163\\446\end{pmatrix} Mod\ 26 = \begin{pmatrix}7\\4\end{pmatrix}$$

$$\begin{pmatrix}167\\505\end{pmatrix} Mod\ 26 = \begin{pmatrix}11\\11\end{pmatrix}$$

$$\begin{pmatrix}114\\360\end{pmatrix} Mod\ 26 = \begin{pmatrix}14\\22\end{pmatrix}$$

$$\begin{pmatrix}114\\381\end{pmatrix} Mod\ 26 = \begin{pmatrix}14\\17\end{pmatrix}$$

$$\begin{pmatrix}245\\679\end{pmatrix} Mod\ 26 = \begin{pmatrix}11\\3\end{pmatrix}$$

d. Ubah setiap matriks angka menjadi hurud dengan aturan konversi seperti tabel 4.1.

$$\begin{pmatrix}7\\4\end{pmatrix} = \begin{pmatrix}H\\E\end{pmatrix}$$

$$\begin{pmatrix}11\\11\end{pmatrix} = \begin{pmatrix}L\\L\end{pmatrix}$$

$$\begin{pmatrix}14\\22\end{pmatrix} = \begin{pmatrix}O\\W\end{pmatrix}$$

$$\begin{pmatrix}14\\17\end{pmatrix} = \begin{pmatrix}O\\R\end{pmatrix}$$

$$\begin{pmatrix}11\\3\end{pmatrix} = \begin{pmatrix}L\\D\end{pmatrix}$$

e. Didapatkan pesan SLHYATGZT yang telah didekripsi menjadi HELLOWORLD dan dapat dengan mudah dimengerti bahwa pesan tersebut adalah HELLO WORLD.

V. KRIPTANALISIS PADA HILL CIPHER

Teknik kriptanalisis terhadap Hill Cipher sangat sulit untuk dilakukan. Terlebih jika dilakukan dengan *ciphertext-only attack* dan matriks kunci yang digunakan berdimensi besar. Kesulitan ini disebabkan oleh *ciphertext* Hill Cipher yang tidak memiliki pola dan setiap karakter dalam satu blok saling mempengaruhi karakter lainnya.

Teknik yang memungkinkan untuk kriptanalisis Hill Cipher adalah *known plaintext attack.* Jika kriptanalisis memiliki pecahan *plaintext* dan *ciphertext* yang saling berkorespondensi, maka Hill Cipher dapat di pecahkan. Namun proses yang harus dilalui cukup sulit, yakni menentukan panjang kunci yang digunakan. Hal ini menjadi salah satu kekuatan yang dimiliki oleh Hill Cipher. Cara satu-satunya adalah dengan mencari tahu panjang kunci atau dengan melakukan perkiraan dan coba-coba. [5]

Misalkan kriptanalis mengetahui panjang kunci K adalah 2 dan memiliki potongan berkas *plaintext* P dan *ciphertext* C sebagai berikut:

P = OF THE
C = FUPCMTGZKYUKBQFJHUKTZKKIXTTA

Dari informasi yang dimiliki, kita tahu bahwa “OF THE” muncul pada pesan yang memiliki *ciphertext* C, namun tidak tahu “OF THE” muncul pada posisi yang mana. Berarti pasti ada keadaan dimana “OF THE” akan menempati posisi yang benar.

Fu	pc	mt	gz	ky	uk	bq	fj	hu	kt	zk	ki	xt	ta
of	th	e.	..	..	..	..	..	..	..	..	..	..	..
.o	ft	he	..	..	..	..	..	..	..	..	..	..	..
..	of	th	e.	..	..	..	..	..	..	..	..	..	..
..	.o	ft	he	..	..	..	..	..	..	..	..	..	..
..	..	of	th	e.	..	..	..	..	..	..	..	..	..
..	..	.o	ft	he	..	..	..	..	..	..	..	..	..
...	..												

Misalkan kita menganggap benar pada baris kedua, didapatkan PC → FT dan MT → HE. Sekarang kita dapat menentukan matriks kunci dari informasi tersebut.

$$P = K^{-1}.C$$

$$\begin{pmatrix}F\\T\end{pmatrix} = K^{-1}.\begin{pmatrix}P\\C\end{pmatrix}$$
$$\begin{pmatrix}5\\19\end{pmatrix} = K^{-1}.\begin{pmatrix}15\\2\end{pmatrix}$$

$$\begin{pmatrix}H\\E\end{pmatrix} = K^{-1}.\begin{pmatrix}7\\4\end{pmatrix}$$
$$\begin{pmatrix}M\\T\end{pmatrix} = K^{-1}.\begin{pmatrix}12\\19\end{pmatrix}$$

Gabungkan kedua matriks diatas menjadi sebuah matriks berukuran 2 x 2.

$$\begin{pmatrix}5 & 7\\19 & 4\end{pmatrix} = K^{-1}.\begin{pmatrix}15 & 12\\2 & 19\end{pmatrix}$$
$$K^{-1} = \begin{pmatrix}5 & 7\\19 & 4\end{pmatrix}\begin{pmatrix}15 & 12\\2 & 19\end{pmatrix}^{-1}$$
$$K^{-1} = \begin{pmatrix}5 & 7\\19 & 4\end{pmatrix}\begin{pmatrix}19 & -12\\-2 & 15\end{pmatrix}$$
$$K^{-1} = \begin{pmatrix}81 & 45\\353 & -168\end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} 3 & 19 \\ 15 & 14 \end{pmatrix} mod\ 26$$

Maka didapatkan matriks kunci deskripsi $K^{-1} = \begin{pmatrix} 3 & 19 \\ 15 & 14 \end{pmatrix}$. Tapi jika kita mendekripsinya maka akan didapatkan pesan berupa

frfthezyssqyvfetlvbafvaconfz

yang berarti bahwa asumsi awal kita yang menganggap benar baris dua (PC → FT dan MT → HE). Untuk mendapat posisi yang tepat kta perlu menggeser dan mencocokan kata "OF THE" dengan *ciphertext* yang diapat sampai terbentuk kata yang dapat dibaca.

Jika kita mengasumsikan benar pada baris 18 dan didapatkan KT →FT dan ZK → HE. Dengan mengulang prosedur untuk memperoleh matriks kunci K^{-1} seperti diatas, didapatkan:

$$K^{-1} = \begin{pmatrix} 17 & 5 \\ 18 & 23 \end{pmatrix} mod\ 26$$

Dan jika dicoba untuk melakukan dekripsi dari *ciphertext* yang dimiliki, didapatkan pesan:

defendtheeastwallofthecastle

VI. KESIMPULAN

Berdasarkan pembahasan yang telah dilakukan, maka kesimpulan yang dapat diambil antara lain:

1. Hill Cipher adalah algoritma kriptogradi klasik yang sangat kuat dilihat dari segi keamanannya.
2. Matriks kunci Hill Cipher harus merupakan matriks *invertible*. Semakin besar matriks kunci, semakin sulit untuk dipecahkan oleh orang lain yang berarti semakin tinggi tingkat kemanannya.
3. Hill Cipher kuat dalam menghadapi *ciphertext only attack* namun lemah jika diserang dengan *known plaintext attack*.

VII. UCAPAN TERIMAKASIH

Penulis pertama-tama ingin mengucpkan syukur kepada Tuhan Yang Maha Esa karena rahmat dan berkat-Nya yang selalu menyertai penulis hingga pembuatan makalah ini selesai. Penulis juga ingin berterima kasih kepada kedua orang tua penulis yang selalu memberi *support* dan semangat kepada penulis. Tak lupa penulis ucapkan terima kasih kepada Bapak Rinaldi Munir dan Bapak Judi karena melalui pengjarannya, penulisa dapat memahami konsep Matematika Distrik termasuk didalamnya teori graf yang menjadi dasar makalah ini..

REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Program Studi Teknik Informatika, Sekolah teknik Elektro dan Informatika, 2006.
[2] Forouzan, Behrouz, *Cryptography and Network Securuty*, McGraw-Hill, 2006.
[3] http://www.experts-exchange.com/articles/12460/Cryptanalysis-and-Attacks.html, diakses pada tanggal 15 Desember 2015, pukul 20.00.
[4] Worthington, Brian, *An Introduction to Hill Ciphers Using Linear Algebra*, University of North Texas, 2010.
[5] http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-hill-cipher/, diakses pada tanggal 15 Desember, pukul 17.00.

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

Adam Rotal Yuliandaru
13514091