KRIPTOGRAFI HILL-CHIPER MENGGUNAKAN MODULAR GANJIL DAN GENAP

Albinur Limbong
Fakultas Teknologi Informasi Universitas Advent Indonesia

Abstrak

Seiring perkembangan teknologi informasi dan komunikasi, salah satu hal yang sangat penting dilakukan adalah mengamankan kerahasiaan suatu data atau informasi. Kriptografi atau informasi. Salah satu metode yang digunakan adalah Hill Chipers, yaitu suatu metode yang mengubah teks asli menjadi teks rahasia atau sebaliknya dengan menggunakan matriks. Hill Cipher merupakan salah satu algoritma kriptografi menggunakan kunci simetriks. Algoritma Hill Cipher menggunakan matriks *invertible* berukuran n x n sebagai kunci untuk melakukan enkripsi, yaitu mengubah teks asli (*plaintext*) menjadi teks rahasia (*chipertext*), atau sebaliknya melakukan dekripsi, yaitu mengubah *chipertext* menjadi *plaintext*. Pada enkripsi teks asli yang telah dikonversi menjadi angka dikalikan dengan matriks enskripsi dan hasil perkalian yang merupakan angka kemudian dikembalikan menjadi huruf rahasia, dan kemudian matriks invers digunakan kemudian untuk mendekripsi *chipertext* menjadi *plaintext*. Karena menggunakan matriks sebagai kunci menyebabkan Hill Cipher sangat sulit dipecahkan. Dalam berbagai referensi teks yang akan dikonversi memiliki panjang 26 alfabet dan matriks yang digunakan adalah dengan modular genap. Namun dalam kenyataan alfabet (karakter) yang akan dikonversi tidak terbatas pada jumlah 26, namun dapat lebih dari 26 dan jumlahnya bisa ganjil, sehingga matriks konversi adalah modular ganjil juga. Artikel ini membahas mengenai dasar kriptografi Hill Cipher menggunakan matriks dengan modular ganjil maupun genap.

Kata-kata kunci: Hill chiper, kriptografi, matriks, enchiper, dechiper.

HILL-CHIPER CRYPTOGRAPHY USING ODD AND EVEN MODULAR

Abstract

Due to the advancement of information and communication technology, securing data or information is one of the important task to do. Cryptography is one of a computational science that develop very fast in order to protect data or information. One of method used in cryptography is Hill chiper, i.e.a methode used to convert plaintext to become chipertext vice versa, by using a matrix. Hill chiper is one of cryptography algorithm using symmetrical keys. Hill chiper algorithm uses an invertible matrix n x n as a key to encrypt, to covert plaintext to become chipertext, or to decrypt, to convert chipertext back to plaintext. For encryption the plaintext, which is converted into number, is multiplied by the enchipering matrix, and the results, which in number, are again converted into texts. Due to the fact that it uses matrix as a key for encryption or decryption, then Hill chiper is very difficult to break. In some references, text to be converted has 26 alphabets and the matrix used to convert is also even modular. In fact, the length of the different texts to be converted is not limited to 26, it can be longer than 26, and the converting matrix can also be odd modular. This paper disscuss the Hill chiper cryptography by using a matrix not only even modular but also odd modular.

Key words: Hill chiper, cryptography, matrix, enchiper, dechiper.

Pendahuluan

Dalam dunia komunikasi, khususnya komunikasi tertulis, salah satu hal yang mendapat perhatian besar adalah kerahasian informasi yang dikomunikasikan tersebut, khususnya jika informasi yang disampaikan tersebut sangat rahasia dan tidak boleh diketahui siapun juga, kecuali pihak penerima informasi tersebut. Namun seiring dengan perkembangan teknologi informasi dan

komunikasi, sangat dimungkinan informasi yang disampaikan disadap 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 menjaga 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 membuat *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. Dalam beberapa referensi (Anton & Rorres, 2005) Metode Hill Chipers menggunakan modular genap (26 dan seterusnya), pada artikel ini akan didiskusikan metode kriptografi Hill Chipers menggunakan matriks dengan modular ganjil (27 dan seterusnya).

Metode Hil Chiper

Kriptografi Hill Cipher adalah sebuah teknik kriptografi klasik yang dibuat oleh Lester S. Hill dan diperkenalkan tahun 1929. Hill cipher termasuk dalam sistem kriptografi polialfabetik dengan menggunakkan 26 huruf dalam bahasa Inggris, yang berkorespodensi dengan angka 0 sampai 25 (Chiper, 1929). Pada dasarnya metode Hill chipers ini adalah mengubah teks menjadi angka, dimana huruf "A" menjadi angka "1", dan seterusnya huruf "Y" menjadi "25", sedangkan huruf "Z" bukan "26" tetapi menjadi "0" dengan tujuan tertentu, seperti tabel berikut ini.

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	V	U	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Proses *Enchipering*

Bila sebuah pesan akan dikodekan menjadi pesan rahasia, maka langkah-langkah yang digunakan adalah sebagai berikut:

1. Mengubah pesan huruf tersebut menjadi angka.
2. Mengelompokkan huruf tersebut atas jumlah kelompok yang sama, misalnya atas dua pasangan karakter. Kelompok pasangan itu kemudian dibuat dalam matriks kolom.
3. Bila jumlah kelompok yang dipilih adalah dua, maka pilihlah sebuah matriks bujursangkar dengan orde 2 x 2, kemudian kalikan matriks tersebut dengan pasangan karakter yang sudah dalam bentuk angka tersebut. Bila jumlah karakter yang akan dikodekan bukan genap, maka huruf terakhir tidak punya pasangan, untuk kasus ini tambahkan saja huruf yang sama dengan yang terakhir tersebut sebagai pasangannya.
4. Hasil perkalian tersebut kemudian dibagi dengan angka "26" dengan cara modular (mod). Hasil pembagian mod adalah sisa dari nilai bulat.

   Sebagai contoh:

   2 mod 26 = 2, (2/26 = 0 sisa 2)

   27 mod 26 = 1, (27/26 = 1 sisa 1)

   26 mod 26 = 0, (26/26 = 1 sisa 0)

   Bagaimana kalau bilangan yang dibagi itu adalah negatif? Maka sisa pembagiannya ditambahkan dengan angka 26.

   Sebagai contoh:

-2 mod 26 = 24 (-2/26 = 0 sisa -2, kemudian -2 + 26 = 24)
-51 mod 26 = 1 (-51/26 = -1 sisa -25, kemudian -25 +26 = 1)
-26 mod 26 = 0 (-26/26 = -1 sisa 0. Khusus untuk ini tidak ditambah dengan 26).

5. Kelompok angka hasil pembagian modular itu kemudian dikembalikan menjadi huruf yang menjadi pesan rahasianya (*chipertext*).

Sebagai contoh jika matriks $\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}$ digunakan untuk mengubah kata: "KRIPTOGRAFI" menjadi pesan rahasia berikut adalah langkah-langkahnya:

1. Mengubah karakter-karakter "KRIPTOGRAFI" menjadi angka, sehingga didapatlah angka: "11 18 9 16 20 15 7 18 1 6 9".
2. Mengelompokkan barisan angka di atas dalam dua pasangan. Karena jumlah karakter adalah ganjil maka ditambahkan angka "9" ke barisan angka di atas. Misalnya matrik kolom untuk pasangan pertama adalah $\begin{bmatrix}11\\18\end{bmatrix}$
3. Mengalikan kelompok angka tersebut dengan matrik di atas. Selanjutnya untuk langkah keempat dan kelima adalah sebagai berikut:

Huruf K dan R: $\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}\begin{bmatrix}11\\18\end{bmatrix} = \begin{bmatrix}47\\54\end{bmatrix} \bmod 26 = \begin{bmatrix}21\\2\end{bmatrix} = \begin{bmatrix}U\\B\end{bmatrix}$

Huruf I dan P: $\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}\begin{bmatrix}9\\16\end{bmatrix} = \begin{bmatrix}41\\48\end{bmatrix} \bmod 26 = \begin{bmatrix}15\\22\end{bmatrix} = \begin{bmatrix}O\\V\end{bmatrix}$

Huruf T dan O: $\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}\begin{bmatrix}20\\15\end{bmatrix} = \begin{bmatrix}50\\45\end{bmatrix} \bmod 26 = \begin{bmatrix}24\\19\end{bmatrix} = \begin{bmatrix}X\\S\end{bmatrix}$

Huruf G dan R: $\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}\begin{bmatrix}7\\18\end{bmatrix} = \begin{bmatrix}43\\54\end{bmatrix} \bmod 26 = \begin{bmatrix}17\\2\end{bmatrix} = \begin{bmatrix}Q\\B\end{bmatrix}$

Huruf A dan F: $\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}\begin{bmatrix}1\\6\end{bmatrix} = \begin{bmatrix}13\\18\end{bmatrix} \bmod 26 = \begin{bmatrix}13\\18\end{bmatrix} = \begin{bmatrix}M\\R\end{bmatrix}$

Dan kelompok yang terakhir adalah:

Huruf I dan I: $\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}\begin{bmatrix}9\\9\end{bmatrix} = \begin{bmatrix}27\\27\end{bmatrix} \bmod 26 = \begin{bmatrix}1\\1\end{bmatrix} = \begin{bmatrix}A\\A\end{bmatrix}$

Sehingga *Plaintext* "KRIPTOGRAFI" akan berubah menjadi *Chipertext* "UBOVXSQBMRA".

Resiprokal (Invers perkalian)

Jika **a** adalah bilangan dalam Z_m, maka sebuah bilangan $\mathbf{a^{-1}}$ dalam Z_m disebut resiprokal atau (invers perkalian) dari **a mod m** jika $\mathbf{aa^{-1}}$ **mod m** = $\mathbf{a^{-1}a}$ **mod m** = 1. Berikut ini diberikan angka-angka pasangan resiprokal modular 26:

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Sebagai contoh, angka 5 dan 21 adalah pasangan resiprokal karena 5 x 21 mod 26 = 1

Proses *Deciphering*

Bila matrik A adalah matriks yang digunakan untuk proses *enciphering*, dan bila matriks B adalah matriks yang digunakan untuk proses *deciphering*, maka matriks A dan B memiliki hubungan:

AB mod 26 = BA mod 26 = I (matriks identitas)

Dari contoh sebelumnya, maka matriks B yang akan digunakan untuk proses *deciphering* pesan *chipertext* tersebut didapat sebagi berikut:

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

Maka

$$B = A^{-1} = (\det(A))^{-1}\begin{bmatrix}3 & -2\\ 0 & 1\end{bmatrix}$$

Det(A) = (3)(1) – (2)(0) = 3, maka resiprokalnya, $(\det(A))^{-1}$, = 9, yaitu pasangan resiprokal dari 3. Sehingga

$$B = 9\begin{bmatrix}3 & -2\\ 0 & 1\end{bmatrix} = \begin{bmatrix}27 & -18\\ 0 & 9\end{bmatrix} \bmod 26 = \begin{bmatrix}1 & 8\\ 0 & 9\end{bmatrix}$$

Maka $B = \begin{bmatrix}1 & 8\\ 0 & 9\end{bmatrix}$

Langkah berikutnya adalah mengembalikan chipertext ”UBOVXSQBMRA” menjadi *plaintext*, dengan cara berikut:

Huruf U dan B: $\begin{bmatrix}1 & 8\\ 0 & 9\end{bmatrix}\begin{bmatrix}21\\ 2\end{bmatrix} = \begin{bmatrix}37\\ 18\end{bmatrix} \bmod 26 = \begin{bmatrix}11\\ 18\end{bmatrix} = \begin{bmatrix}K\\ R\end{bmatrix}$

Huruf O dan V: $\begin{bmatrix}1 & 8\\ 0 & 9\end{bmatrix}\begin{bmatrix}15\\ 22\end{bmatrix} = \begin{bmatrix}191\\ 198\end{bmatrix} \bmod 26 = \begin{bmatrix}9\\ 16\end{bmatrix} = \begin{bmatrix}I\\ P\end{bmatrix}$

Huruf X dan S: $\begin{bmatrix}1 & 8\\ 0 & 9\end{bmatrix}\begin{bmatrix}24\\ 19\end{bmatrix} = \begin{bmatrix}176\\ 171\end{bmatrix} \bmod 26 = \begin{bmatrix}20\\ 15\end{bmatrix} = \begin{bmatrix}T\\ O\end{bmatrix}$

Huruf Q dan B: $\begin{bmatrix}1 & 8\\ 0 & 9\end{bmatrix}\begin{bmatrix}17\\ 2\end{bmatrix} = \begin{bmatrix}33\\ 18\end{bmatrix} \bmod 26 = \begin{bmatrix}7\\ 18\end{bmatrix} = \begin{bmatrix}G\\ R\end{bmatrix}$

Huruf M dan R: $\begin{bmatrix}1 & 8\\ 0 & 9\end{bmatrix}\begin{bmatrix}13\\ 18\end{bmatrix} = \begin{bmatrix}157\\ 162\end{bmatrix} \bmod 26 = \begin{bmatrix}1\\ 6\end{bmatrix} = \begin{bmatrix}A\\ F\end{bmatrix}$

Dan yang terakhir

Huruf A dan A: $\begin{bmatrix}1 & 8\\ 0 & 9\end{bmatrix}\begin{bmatrix}1\\ 1\end{bmatrix} = \begin{bmatrix}9\\ 9\end{bmatrix} \bmod 26 = \begin{bmatrix}9\\ 9\end{bmatrix} = \begin{bmatrix}I\\ I\end{bmatrix}$

Dengan demikian hasil *deciphering* adalah: KRIPTOGRAFI (yang adalah teks asalnya).

Memecahkan Hill Chiper

Salah satu tugas kriprografer, adalah membuat kode kriptografi sehingga pesan rahasia tidak dapat dibaca oleh musuh (yang tidak berkepentingan). Untuk itu proses/metode *chipering* harus dibuat sedemikian rupa hingga sulit (mustahil) untuk dipecahkan oleh musuh, walau sebagus apapun metode tersebut tetap saja ada peluang untuk memecahkannya. Pada pembahasan berikut ini akan dijelaskan bagaimana memecahkan suatu pesan rahasia yang dikodekan dengan metode Hill Chiper.

Untuk memecahkan Hill chiper, pertama-tama harus ada gambaran apakah kata-kata awal yang umum yang digunakan dalam surat. Misalnya kata ”Dear Sir”, ”Apa kabar”, dst. Bila pesan rahasia itu dibentuk dengan matriks 2x2 (2-chiper), maka dibutuhkan paling tidak empat huruf yang diterka adalah pesan aslinya.

Kemudian, dibentuk matrik untuk pesan rahasia sebagai berikut: $C = \begin{bmatrix}C_1^T\\ C_2^T\end{bmatrix}$, dimana C_1^T adalah matriks transpose dari dua angka pesan rahasia pertama, sedangkan C_2^T adalah matriks transpose dari dua angka pesan rahasia kedua. Kemudian dibentuk juga matriks untuk empat huruf terkaan (yang dianggap *plaintext*): $P = \begin{bmatrix}P_1^T\\ P_2^T\end{bmatrix}$, dimana P_1^T adalah matriks transpose dari dua angka pesan terkaan pertama, sedangkan P_2^T adalah matriks transpose dari dua angka pesan terkaan kedua. Langkah berikutnya, kedua matriks P dan C digabung menjadi matriks augmented $[C \mid P]$.

Kemudian pada matriks augmented $[C \mid P]$ dilakukan proses eliminasi Gauss-Jordan, sehingga bagian C menjadi identitas, sehingga matriks P yang telah mengalami proses eliminasi akan berubah menjadi **matriks *deciphering***. Perlu dicatat bahwa pada proses eliminasi, perlu dipahami konsep angka resiprokal dan pembagian modular 26.

Sebagai contoh, dimisalkan dilakukan penyadapan terhadap pesan terkirim dengan pesan rahasia.

IOSBTGXESPXHOPDE

Dimana diterka bahwa empat huruf pertama adalah "DEAR".

Berikut ini diberikan langkah-langkah menyelesaikan chipertext tersebut:

1. Pertama adalah menentukan matriks decipheringnya untuk terkaan kata "DEAR".Dengan mengkonversi empat huruf pertama dari pesan rahasia dan pesan terkaan menjadi angka didapatlah matriks C dan P sebagai berikut:

   $$P = \begin{bmatrix} 4 & 5 \\ 1 & 18 \end{bmatrix} \text{ dan } C = \begin{bmatrix} 9 & 15 \\ 19 & 2 \end{bmatrix}$$

2. Kemudian matriks C dan P digabungkan menjadi matriks *augmented* (C|P*)*, dan selanjutnya dilakukan proses eliminasi dengan langkah-langkah sebagai berikut:

2.1 Membentuk matriks augmented [C|P]

$$\left[\begin{array}{cc|cc} 9 & 15 & 4 & 5 \\ 19 & 2 & 1 & 18 \end{array}\right]$$

2.2 Mengalikan baris pertama dengan 9^{-1}=3, agar elemen pertama = 1, tetapi elemen lain dikalikan dengan resiprokalnya yaitu 3, agar tidak muncul bilangan pecahan.

$$\left[\begin{array}{cc|cc} 1 & 45 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right]$$

2.3 Mengubah angka 45 menjadi angka kurang dari 26 dengan cara 45 mod 26 = 19.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right]$$

2.4 Mengeliminasi angka 19 pada baris kedua sehingga menjadi 0, dengan cara mengalikan baris pertama dengan -19 dan menambahkannya dengan baris kedua, dan hasilnya dibuat pada baris kedua.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & -359 & -227 & -267 \end{array}\right]$$

2.5 Mengubah angka pada baris kedua dengan angka < 26, dengan pembagian modular.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 5 & 7 & 19 \end{array}\right]$$

2.6. Mengubah angka 5 pada baris dua menjadi 1 dengan mengalikan 5^{-1} = 21.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 1 & 147 & 399 \end{array}\right]$$

2.7. Mengkonversi angka yang > 26 menjadi lebih kecil dari 26.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 1 & 17 & 9 \end{array}\right]$$

2.8. Mengalikan baris kedua dengan -19 dan tambahkan dengan baris pertama. Tujuannya agar elemen kedua baris pertama menjadi 0, agar terbentuk matrik identitas untuk C.

$$\left[\begin{array}{cc|cc} 1 & 0 & -311 & -156 \\ 0 & 1 & 17 & 9 \end{array}\right]$$

2.9. Mengkonversi angka -311 dan -156 menjadi 1 dan 0 dengan prinsip mod.

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 17 & 9 \end{array}\right]$$

2.10. Matriks Deciphering adalah transpose dari matriks P di atas, yaitu

$$P^T = \begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}$$

3. Langkah terakhir adalah mengkonversi pesan rahasia: "IOSBTGXESPXHOPDE" menjadi plaintext, dengan langkah-langkah berikut:

3.1. Mengganti huruf dengan angka dengan dan dikelompokkan atas dua huruf:

I OS B	T G	X E	S P	X H	O P	D E	
9 15	19 2	20 7	24 5	19 16	24 8	15 16	4 5

3.2. Mengalikan pasangan-pasangan di atas dengan matriks deciphering, dan mengembalikan angka tersebut menjadi huruf.

I dan O: $\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 9 \\ 15 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} D \\ E \end{bmatrix}$

S dan B: $\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 19 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 18 \end{bmatrix} = \begin{bmatrix} A \\ R \end{bmatrix}$

T dan G: $\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 20 \\ 7 \end{bmatrix} = \begin{bmatrix} 9 \\ 11 \end{bmatrix} = \begin{bmatrix} I \\ K \end{bmatrix}$

X dan E: $\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 24 \\ 5 \end{bmatrix} = \begin{bmatrix} 5 \\ 19 \end{bmatrix} = \begin{bmatrix} E \\ S \end{bmatrix}$

S dan P: $\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 19 \\ 16 \end{bmatrix} = \begin{bmatrix} 5 \\ 14 \end{bmatrix} = \begin{bmatrix} E \\ N \end{bmatrix}$

X dan H: $\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 24 \\ 8 \end{bmatrix} = \begin{bmatrix} 4 \\ 20 \end{bmatrix} = \begin{bmatrix} D \\ T \end{bmatrix}$

O dan P: $\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 1 \\ 14 \end{bmatrix} = \begin{bmatrix} A \\ N \end{bmatrix}$

D dan E: $\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 11 \\ 19 \end{bmatrix} = \begin{bmatrix} K \\ S \end{bmatrix}$

Maka teks asli (*plaintext*) adalah: DEAR IKE SEND TANKS

Hill Chiper dengan modular Ganjil

Dari pembahasan di atas, panjang teks yang akan dikonversi adalah 26, sehingga hasil perkalian matriks enchipering dengan teks asli dibagi dengan 26 (modular genap). Kemudian pasangan resiprokal **a** dan $\mathbf{a^{-1}}$ yang digunakan untuk menentukan matriks dechiperingnya adalah pasangan angka ganjil. Hasil determinan dari matriks *enchipering* tidak selalu ganjil, sehingga pasangan resiprokalnya sudah pasti bukan ganjil jika menggunakan modular ganjil. Sebagai contoh, kalau matriks enchiperingnya adalah

$$A = \begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix},$$

maka determinan (A) adalah 2 (genap), sehingga tidak memiliki pasangan resiprokal ($\mathbf{a^{-1}}$) jika menggunakan modular 26. Untuk itu harus menggunakan modular ganjil (27 atau lebih).
Pasangan resiprokal untuk bilangan genap, menggunakan modular ganjil 27 adalah:

A	1	2	4	5	7	8	10	…
a^{-1}	1	14	7	11	4	17	19	…

Jika matriks A di atas digunakan untuk mengubah *plaintext*: LOVE (L=12, O=15, V=22 dan E=5), maka akan didapat

Huruf L dan O: $\begin{bmatrix}1 & 3\\0 & 2\end{bmatrix}\begin{bmatrix}12\\15\end{bmatrix}=\begin{bmatrix}57\\30\end{bmatrix}\bmod 27=\begin{bmatrix}3\\3\end{bmatrix}=\begin{bmatrix}C\\C\end{bmatrix}$

Huruf V dan E: $\begin{bmatrix}1 & 3\\0 & 2\end{bmatrix}\begin{bmatrix}22\\5\end{bmatrix}=\begin{bmatrix}37\\10\end{bmatrix}\bmod 27=\begin{bmatrix}10\\10\end{bmatrix}=\begin{bmatrix}J\\J\end{bmatrix}$

Maka *chipertext* nya adalah: **CCJJ**.

Selanjutnya jika pesan rahasia di atas ingin dikembalikan menjadi pesan asli, maka terlebih dahulu dicari matriks *dechipering*nya (B) sebagai berikut.

$B = A^{-1} = (\det(A))^{-1}\begin{bmatrix}2 & -3\\0 & 1\end{bmatrix}=14\begin{bmatrix}2 & -3\\0 & 1\end{bmatrix}=\begin{bmatrix}28 & -42\\0 & 14\end{bmatrix}\bmod 27=\begin{bmatrix}1 & 12\\0 & 14\end{bmatrix}$

Selanjutnya pesan CCJJ diubah sebagai berikutnya:

Huruf C dan C: $\begin{bmatrix}1 & 12\\0 & 14\end{bmatrix}\begin{bmatrix}3\\3\end{bmatrix}=\begin{bmatrix}39\\42\end{bmatrix}\bmod 27=\begin{bmatrix}12\\15\end{bmatrix}=\begin{bmatrix}L\\O\end{bmatrix}$

Huruf J dan J: $\begin{bmatrix}1 & 12\\0 & 14\end{bmatrix}\begin{bmatrix}10\\10\end{bmatrix}=\begin{bmatrix}130\\140\end{bmatrix}\bmod 27=\begin{bmatrix}22\\5\end{bmatrix}=\begin{bmatrix}V\\E\end{bmatrix}$

Hasilnya adalah pesan asli "**LOVE**".

Kesimpulan

Dari penjelasan di atas diambil kesimpulan bahwa Hill chiper dapat digunakan bukan saja untuk matriks dengan modular 26 (genap), tetapi juga matriks dengan modular 27 (ganjil) atau bilangan ganji lainnya. Pilihan modular ini tergantung kepada jumlah teks yang berbeda yang akan di*enchiper*, atau juga bergantung kepada determinan dari matriks yang digunakan untuk melakukan *enchipering*. Bila determinan matriks *enchipering* adalah ganjil maka digunakan modular genap, dan bila matriks *enchipering* adalah genap maka digunakan modular ganjil. Bilamana Hill chiper digunakan untuk memecahkan suatu pesan rahasia maka aturan yang sama juga digunakan, bahwa jika teks terkaan menghasilkan matriks yang determinannya adalah genap maka digunakan modular ganjil (27 atau angka ganjil yang lain), dan bilamana determinannya adalah ganjil maka digunakan genap (26 atau angka genap lainnya).

Referensi

1. Anton, H. & C. Rorres, (2005), Elementary Linear Algebra with Applications, John Wiley and Sons, Inc., New York, NY, pp. 719-732
2. Hill, L.S., (1929), Cryptography in an Algebraic Alphabet: *The American Mathematical Monthly*, 36 (6), pp.306-312.
3. Worthington, B, (2010) An Introduction to Hill Ciphers Using Linear Algebra, University of Northern Texas, http://davinci.cascss.unt.edu/users/tushar/S10Linear2700%20%20Project_files/Worthington%20Paper.pdf.