Studi dan Analisis mengenai Hill Cipher, Teknik Kriptanalisis dan Upaya Penanggulangannya

Arya Widyanarko
Program Studi Teknik Informatika, Institut Teknologi Bandung, Jl. Ganesha 10 Bandung
Email: if14030@students.if.itb.ac.id

Abstract *– Hill cipher merupakan salah satu algoritma kriptografi kunci simetris. Algoritma Hill cipher menggunakan matriks berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks.*

Karena menggunakan matriks sebagai kunci, Hill cipher merupakan algoritma kriptografi kunci simetris yang sulit dipecahkan, karena teknik kriptanalisis seperti analisis frekuensi tidak dapat diterapkan dengan mudah untuk memecahkan algoritma ini. Hill cipher sangat sulit dipecahkan jika kriptanalis hanya memiliki ciphertext saja (chipertext-only), namun dapat dipecahkan dengan mudah jika kriptanalis memiliki ciphertext dan potongan dari plaintext-nya (known-plaintext).

Makalah ini membahas mengenai dasar teori Hill cipher, teknik kriptanalis yang dapat dilakukan untuk memecahkan Hill cipher dan upaya dalam memodifikasi Hill cipher. Modifikasi yang dilakukan untuk meningkatkan keamanan algoritma kriptografi kunci simetris ini agar kriptanalis tidak dapat memecahkan kunci algoritma Hill cipher.

Kata Kunci*: Hill cipher, known-plaintext attack, Matriks, Matriks identitas.*

1. PENDAHULUAN

Hill cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi.

Hill cipher diciptakan oleh Lester S. Hill pada tahun 1929 [3]. Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan *cipher* yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Berbeda dengan *caesar cipher*, *hill cipher* tidak mengganti setiap abjad yang sama pada plainteks dengan abjad lainnya yang sama pada cipherteks karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.

Hill cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas cipherteks saja.

Namun, teknik ini bukan berarti tanpa cela, *hill cipher* dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas cipherteks dan potongan berkas plainteks. Teknik kriptanalisis ini disebut *known-plaintext attack* [4].

2. HILL CIPHER

Hill cipher yang merupakan *polyalphabetic cipher* dapat dikategorikan sebagai *block cipher* [2] 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.

2.1. Dasar teori

Dasar dari teknik *hill cipher* adalah aritmatika modulo terhadap matriks. Dalam penerapannya, *hill cipher* menggunakan teknik perkalian matriks dan teknik invers terhadap matriks.

Kunci pada *hill cipher* adalah matriks *n* x *n* dengan *n* merupakan ukuran blok. Jika matriks kunci kita sebut dengan *K*, maka matriks *K* adalah sebagai berikut :

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mn} \end{bmatrix}$$

Matriks *K* yang menjadi kunci ini harus merupakan matriks yang *invertible*, yaitu memiliki *multiplicative inverse* K^{-1} sehingga :

$$K \,.\, K^{-1} = 1 \qquad (1)$$

Kunci harus memiliki invers karena matriks K^{-1} tersebut adalah kunci yang digunakan untuk melakukan dekripsi.

2.2. Teknik enkripsi

Proses enkripsi pada *hill cipher* dilakukan per blok plainteks. Ukuran blok tersebut sama dengan ukuran matriks kunci. Sebelum membagi teks menjadi deretan

blok-blok, plainteks terlebih dahulu dikonversi menjadi angka, masing-masing sehingga A=0, B=1, hingga Z=25.

Secara matematis, proses enkripsi pada *hill cipher* adalah:

$$C = K \,.\, P \qquad (2)$$

C = Cipherteks
K = Kunci
P = Plainteks
Jika terdapat plainteks P:

P = B E S O K M A L A M
Maka plainteks tersebut dikonversi menjadi:

P = 1 4 18 14 10 12 0 11 0 12
Plainteks tersebut akan dienkripsi dengan teknik *hill cipher*, dengan kunci K yang merupakan matriks 2x2.

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

Karena matriks kunci K berukuran 2, maka plainteks dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter. Blok pertama dari plainteks P adalah :

$$P_{1,2} = \begin{bmatrix} 1 \\ 4 \end{bmatrix}$$

Blok plainteks ini kemudian dienkripsi dengan kunci K melalui persamaan (2).

$$C_{1,2} = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \end{bmatrix} = \begin{bmatrix} 9 \\ 7 \end{bmatrix}$$

Karakter yang berkorespondensi dengan 9 dan 7 adalah J dan H. Maka karakter BE pada plainteks berubah menjadi karakter JH pada cipherteks.

Pada contoh karakter ketiga dan keempat, hasil perhitungan menghasilkan angka yang tidak berkorespondensi dengan huruf-huruf, maka lakukan modulo 26 pada hasil tersebut.

$$C_{3,4} = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 18 \\ 14 \end{bmatrix} = \begin{bmatrix} 46 \\ 68 \end{bmatrix} (\text{mod}\, 26) \equiv \begin{bmatrix} 20 \\ 16 \end{bmatrix}$$

Maka karakter yang berkorespondensi dengan 20 dan 16 adalah U dan Q.

Setelah melakukan enkripsi semua blok pada plainteks P maka dihasilkan cipherteks C sebagai berikut:

P = B E S O K M A L A M
C = J H U Q I Q W L Y M

Dari cipherteks yang dihasilkan terlihat bahwa *hill cipher* menghasilkan cipherteks yang tidak memiliki pola yang mirip dengan plainteksnya.

2.3. Teknik 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 (2).

$$\begin{aligned} C &= K.P \\ K^{-1}.C &= K^{-1}.K.P \\ K^{-1}.C &= 1.P \\ P &= K^{-1}.C \end{aligned}$$

Menjadi persamaan proses dekripsi:

$$P = K^{-1}.C \qquad (3)$$

Dengan menggunakan kunci $K = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$, maka proses dekripsi diawali dengan menghitung invers dari matriks K dengan menggunakan metode operasi baris (*row operation*) [5].

$$\begin{aligned} [K \mid I] &= \left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 1 & 0 & 1 \end{array}\right] (9 \times R2) \\ &= \left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 27 & 9 & 0 & 9 \end{array}\right] (\text{mod}\, 26) \\ &\equiv \left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 1 & 9 & 0 & 9 \end{array}\right] (R2 - R1) \\ &= \left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 7 & -1 & 9 \end{array}\right] (15 \times R2) \\ &= \left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 105 & -15 & 135 \end{array}\right] (\text{mod}\, 26) \\ &\equiv \left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 1 & -15 & 5 \end{array}\right] (R1 - 2R2) \\ &= \left[\begin{array}{cc|cc} 1 & 0 & 31 & -10 \\ 0 & 1 & -15 & 5 \end{array}\right] (\text{mod}\, 26) \\ &= \left[\begin{array}{cc|cc} 1 & 0 & 5 & 16 \\ 0 & 1 & 11 & 5 \end{array}\right] \end{aligned}$$

Setelah melakukan perhitungan, didapat matriks K^{-1} yang merupakan invers dari matriks K, yaitu :

$$K^{-1} = \begin{bmatrix} 5 & 16 \\ 11 & 5 \end{bmatrix}$$

Kunci K^{-1} yang digunakan untuk melakukan dekripsi ini telah memenuhi persamaan (1) karena:

$$\begin{aligned} K.K^{-1} &= \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 5 & 16 \\ 11 & 5 \end{bmatrix} \\ &= \begin{bmatrix} 27 & 26 \\ 26 & 53 \end{bmatrix} \text{mod}\, 26 \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \end{aligned}$$

Cipherteks C = J H U Q I Q W L Y M, akan didekripsi dengan menggunakan kunci dekripsi K^{-1}

dengan persamaan (3). Proses dekripsi ini dilakukan blok per blok seperti pada proses enkripsi.

Pertama-tama ubah huruf-huruf pada cipherteks menjadi urutan numerik.
C = 9 7 20 16 8 16 22 11 24 12

Proses dekripsi dilakukan sebagai berikut:

Blok pertama:

$$P_{1,2} = K^{-1}.C_{1,2}$$
$$= \begin{bmatrix} 5 & 16 \\ 11 & 5 \end{bmatrix}\begin{bmatrix} 9 \\ 7 \end{bmatrix} = \begin{bmatrix} 157 \\ 134 \end{bmatrix} \bmod 26 \equiv \begin{bmatrix} 1 \\ 4 \end{bmatrix}$$

Blok kedua:

$$P_{3,4} = K^{-1}.C_{3,4}$$
$$= \begin{bmatrix} 5 & 16 \\ 11 & 5 \end{bmatrix}\begin{bmatrix} 20 \\ 16 \end{bmatrix} = \begin{bmatrix} 356 \\ 300 \end{bmatrix} \bmod 26 \equiv \begin{bmatrix} 18 \\ 14 \end{bmatrix}$$

Setelah semua blok selesai didekripsi, maka didapatkan hasil plainteks:

P = 1 4 18 14 10 12 0 11 0 12
P = B E S O K M A L A M

3. TEKNIK KRIPTANALISIS TERHADAP HILL CIPHER

Kriptanalisis terhadap *hill cipher* sangat sulit jika dilakukan dengan *ciphertext-only attack*, terlebih apabila matriks kunci yang digunakan berukuran besar. Kesulitan ini disebabkan oleh cipherteks *hill cipher* yang tidak memiliki pola dan setiap karakter dalam satu blok saling mempengaruhi karakter lainnya.

Teknik yang dapat digunakan untuk melakukan kriptanalisis terhadap *hill cipher* adalah *known-plaintext attack*. Jika kriptanalisis memiliki pecahan plainteks dan cipherteks yang saling berkorespondensi, maka *hill cipher* dapat dipecahkan.

Namun proses yang cukup sulit adalah untuk menentukan panjang kunci yang digunkan. Hal ini menjadi salah satu kekuatan yang dimiliki oleh *hill cipher*. Cara yang dapat dilakukan hanya dengan mencari tahu panjang kunci atau dengan melakukan perkiraan dan percobaan.

Kemungkinan terburuk yang dimiliki oleh *hill cipher* adalah ketika seorang kriptanalis memiliki potongan plainteks dan cipherteks yang berkorespondensi serta mengetahui panjang kunci yang digunakan. Dengan informasi ini, kriptanalis dapat memecahkan *hill cipher* dengan sangat mudah.

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

P = B E S O
C = J H U Q I Q W L Y M

Dari informasi yang dimiliki, maka diketahui bahwa karakter BE pada plainteks berkorespondensi dengan karakter JH, dan karakter SO dengan UQ.

Proses pemecahan *hill cipher* ini dapat dilakukan dengan 2 metode, menggunakan perkalian matriks dan menggunakan persamaan linier.

3.1. Perkalian matriks

Dari persamaan (2) dapat kita turunkan rumus untuk menghitung kunci *K*, yaitu:

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

Metode perkalian matriks ini dapat dilakukan jika jumlah blok plainteks yang diketahui sama atau lebih besar dibanding ukuran kunci dan matriks *P* yang berisi blok-blok plainteks tersebut memiliki invers.

Potongan plainteks pada contoh berukuran 2 blok dapat dibentuk menjadi matriks *P*

$$P = \begin{bmatrix} B & S \\ E & O \end{bmatrix} = \begin{bmatrix} 1 & 18 \\ 4 & 14 \end{bmatrix}$$

2 blok cipherteks yang berkorespondensi dengan 2 blok plainteks tersebut dapat dibentuk menjadi matriks *C* sebagai berikut:

$$C = \begin{bmatrix} J & U \\ H & Q \end{bmatrix} = \begin{bmatrix} 9 & 20 \\ 7 & 16 \end{bmatrix}$$

Matriks *P* diatas adalah matriks *invertible*. Dengan melakukan perhitungan menggunakan metode operasi baris (*row operation)* [5], maka didapatkan invers dari *P* adalah:

$$P^{-1} = \begin{bmatrix} 15 & 16 \\ 5 & 15 \end{bmatrix}$$

Dengan menerapkan persamaan (4), maka kriptanalis akan mendapatkan kunci enkripsi *K*:

$$K = C.P^{-1}$$
$$K = C.P^{-1}$$
$$= \begin{bmatrix} 9 & 20 \\ 7 & 16 \end{bmatrix}\begin{bmatrix} 15 & 16 \\ 5 & 15 \end{bmatrix}$$
$$= \begin{bmatrix} 235 & 444 \\ 185 & 352 \end{bmatrix} \bmod 26$$
$$\equiv \begin{bmatrix} 1 & 2 \\ 3 & 14 \end{bmatrix}$$

Dengan melakukan invers terhadap *K* menggunakan metode operasi baris (*row operation*)[5], maka kriptanalis mendapatkan K^{-1} sebagai kunci dekripsi:

$$K^{-1} = \begin{bmatrix} 5 & 16 \\ 11 & 5 \end{bmatrix}$$

Dengan kunci dekripsi yang dimiliki, kriptanalis hanya perlu menerapkan persamaan (3) pada cipherteks dan kunci, sehingga menghasilkan plainteks *P*:

P = B E S O K M A L A M

3.2. Persamaan linier

Pada perkalian matriks, jika matriks yang merepresentasikan plainteks tidak memiliki invers maka pencarian kunci tidak dapat dilakukan.

Namun, dengan menggunakan persamaan linier, maka kunci tersebut akan dapat ditemukan oleh kriptanalis. Metoda ini menggunakan persamaan linier sebagai dasar teorinya.

Misalkan kunci direpresentasikan dengan:

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Plainteks *P* dengan:

$$P = \begin{bmatrix} B & S \\ E & O \end{bmatrix} = \begin{bmatrix} 1 & 18 \\ 4 & 14 \end{bmatrix}$$

Cipherteks *C* dengan:

$$C = \begin{bmatrix} J & U \\ H & Q \end{bmatrix} = \begin{bmatrix} 9 & 20 \\ 7 & 16 \end{bmatrix}$$

Dengan menerapkan persamaan (2) maka persamaan linier yang dapat dibentuk dari contoh adalah:

$$C = K.P$$

$$\begin{bmatrix} 9 & 20 \\ 7 & 16 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 18 \\ 4 & 14 \end{bmatrix}$$

$$9 = a + 4b$$
$$\Leftrightarrow a = 9 - 4b \quad \text{(i)}$$

$$20 = 18a + 14b \qquad \text{(ii)}$$

$$7 = c + 4d$$
$$\Leftrightarrow c = 7 - 4d \qquad \text{(iii)}$$

$$16 = 18c + 14d \qquad \text{(iv)}$$

Dengan melakukan substitusi persamaan (i) ke persamaan (ii) dan persamaan (iii) ke persamaan (iv), maka nilai *a, b, c,* dan *d* dapat dihitung.

$$20 = 18a + 14b$$
$$\Leftrightarrow \quad 20 = 18(9 - 4b) + 14b$$
$$\Leftrightarrow \quad 20 = (162 - 72b) + 14b$$
$$\Leftrightarrow \quad 20 = 162 - 58b$$
$$\Leftrightarrow \quad 58b \pmod{26} = 142 \pmod{26}$$
$$\Leftrightarrow \quad 6b = 12$$
$$\Leftrightarrow \quad b = 2$$

$$16 = 18c + 14d$$
$$\Leftrightarrow \quad 16 = 18(7 - 4d) + 14d$$
$$\Leftrightarrow \quad 16 = (126 - 72d) + 14d$$
$$\Leftrightarrow \quad 16 = 126 - 58d$$
$$\Leftrightarrow \quad 58d \pmod{26} = 110 \pmod{26}$$
$$\Leftrightarrow \quad 6d = 6$$
$$\Leftrightarrow \quad d = 1$$

$$a = 9 - 4b$$
$$\Leftrightarrow \quad a = 9 - 4(2)$$
$$\Leftrightarrow \quad a = 1$$

$$c = 7 - 4d$$
$$\Leftrightarrow \quad c = 7 - 4(1)$$
$$\Leftrightarrow \quad c = 3$$

Dengan nilai *a,b,c* dan *d* maka kunci *K* didapatkan, yaitu:

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

Dengan kunci *K* tersebut, kriptanalis hanya perlu melakukan dekripsi terhadap cipherteks keseluruhan untuk mendapatkan plainteks seutuhnya.

Secara umum, penggunaan metode persamaan linier lebih mudah dan lebih cepat jika dibandingkan dengan perkalian matriks.

4. UPAYA PENANGGULANGAN TERHADAP TEKNIK KRIPTANALISIS

Teknik kriptanalisis dengan *known-plaintext attack* terbukti dapat memecahkan *hill cipher* dengan mudah jika ukuran kunci telah diketahui atau ukuran kunci yasng digunakan kecil.

Upaya pencegahan agar *hill cipher* tidak dapat dipecahkan atau tidak mudah dipecahkan yang paling sederhana adalah menggunakan ukuran matriks kunci yang besar. Semakin besar ukuran matriks kunci, maka semakin sulit *hill cipher* tersebut dipecahkan karena ketergantungan satu karakter dengan karakter lainnya semakin kuat.

Penggunaan matriks kunci berukuran besar memang cukup efektif untuk meningkatkan keamanan cipherteks, namun semakin besar ukuran kunci, maka semakin sulit untuk diingat.

Untuk mempersulit pemecahan *hill cipher*, maka dalam makalah ini penulis melakukan modifikasi terhadap *hill cipher* yang diberi nama *chaining hill cipher*. Modifikasi yang dilakukan adalah pada proses enkripsi dan dekripsi blok cipherteks yang dihasilkan akan dipengaruhi blok plainteks sebelumnya.

Bab ini menjelaskan mengenai perubahan yang dilakukan oleh penulis terhadap *hill cipher* menjadi *chaining hill cipher*.

4.1. Penggunaan matriks dalam Z_{29}

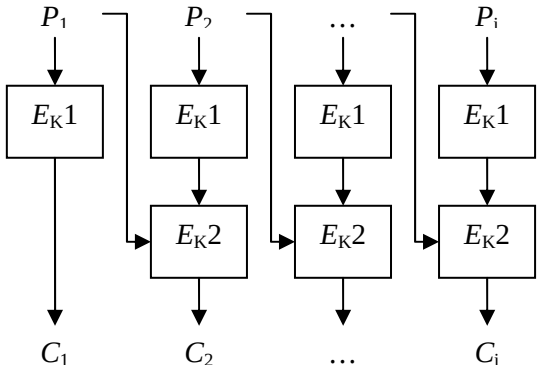
Perubahan dasar yang dilakukan adalah dengan menambah jumlah karakter dari 26 menjadi 29 karakter dengan penambahan karakter spasi, titik dan koma.

Perubahan ini bertujuan untuk memperbanyak kemungkinan matriks yang muncul, karena matriks yang *invertible* dalam Z_{29} lebih banyak dibandingkan Z_{26}. Hal ini disebabkan 29 adalah bilangan prima.

Dengan perubahan jumlah karakter yang diproses, maka operasi modulo yang diterapkan pada *chaining hill cipher* ini adalah modulo terhadap angka 29.

4.2. Proses Enkripsi

Proses enkripsi pada *chaining hill cipher* dapat digambarkan sebagai berikut:



Gambar 1. Proses Enkripsi pada *chaining hill cipher*

E_K1 adalah proses Enkripsi pertama dengan melakukan proses enkripsi *hill cipher* biasa dengan persamaan (2). E_K2 adalah proses tambahan yang melibatkan matriks kunci dan blok plainteks sebelumnya.

Langkah-langkah enkripsi *chaining hill cipher* dijelaskan dalam contoh berikut:

P = B E S O K M A L A M .
P = 1 4 18 14 10 26 12 0 11 0 12 27

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

Hitung *D(K)* yang merupakan determinan dari matriks kunci *K*. Jika nilai *D(K)* mod2 adalah 1, maka nilai *i*=1, jika nilai *D(K)* mod2 adalah 0, maka nilai *i*=-1.

$$\begin{aligned} D(K) &= ad - bc \\ &= -5 \\ D(K) \bmod 2 &= 1 \\ i &= 1 \end{aligned}$$

Lakukan proses enkripsi *hill cipher* biasa (E_K1) pada blok pertama plainteks.

$$P_{1,2} = \begin{bmatrix} 1 \\ 4 \end{bmatrix}$$

$$C_{1,2} = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \end{bmatrix} = \begin{bmatrix} 9 \\ 7 \end{bmatrix}$$

Lakukan proses E_K1 pada blok kedua.

$$E_K1(P_{3,4}) = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 18 \\ 14 \end{bmatrix} = \begin{bmatrix} 46 \\ 68 \end{bmatrix} (\text{mod } 29) \equiv \begin{bmatrix} 17 \\ 10 \end{bmatrix}$$

Jika matriks kunci *K* berukuran *mxm*, Hitung *n* dengan menggunakan *P* dari blok plainteks sebelumnya.

$$\begin{aligned} n &= ((P_1 + P_2) \bmod m) + 1 \\ n &= ((P_1 + P_2) \bmod m) + 1 \\ &= ((1+4) \bmod 2) + 1 \\ &= 2 \end{aligned}$$

Kemudian matriks *Z* adalah matriks kolom ke-*n* dari kunci *K*.

$$Z = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

Lakukan proses enkripsi E_K2 terhadap blok kedua plainteks.

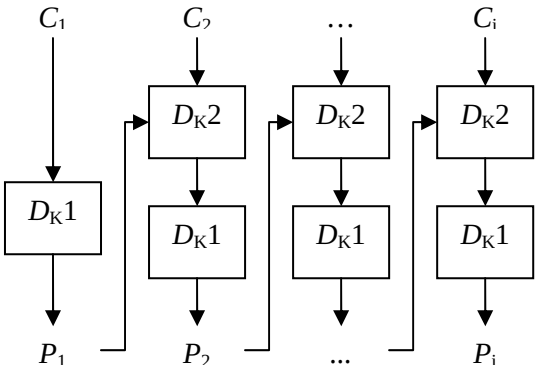
$$\begin{aligned} C_{3,4} &= E_K1(P_{3,4}) + (i.Z) \\ &= \begin{bmatrix} 17 \\ 10 \end{bmatrix} + 1 \begin{bmatrix} 2 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} 19 \\ 11 \end{bmatrix} \end{aligned}$$

Ulangi proses E_K1 dan E_K2 pada seluruh blok yang tersisa. Maka akan menghasilkan cipherteks:

C = 9 7 19 11 5 1 13 10 12 7 10 6
C = J H T L F B N K M H K G

4.3. Proses Dekripsi

Proses dekripsi pada *chaining hill cipher* adalah:



Gambar 2. Proses Dekripsi pada *chaining hill cipher*

D_K1 adalah proses dekripsi *hill cipher* biasa dengan persamaan (3), sementara D_K2 adalah proses yang ditambahkan pada *chaining hill cipher* untuk mengimbangi proses E_K2 pada proses enkripsi.

Langkah-langkah dekripsi *chaining hill cipher* dijelaskan dalam contoh berikut:

C = J H T L F B N K M H K G

C = 9 7 19 11 5 1 13 10 12 7 10 6

$$K = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}, \qquad K^{-1} = \begin{bmatrix} 23 & 12 \\ 18 & 23 \end{bmatrix}$$

K^{-1} didapatkan dengan melakukan invers pada kunci K pada Z_{29} (dengan modulo 29).

Lakukan dekripsi *hill cipher* biasa pada blok cipherteks pertama dengan persamaan (3).

$$P_{1,2} = K^{-1}.C_{1,2}$$
$$= \begin{bmatrix} 23 & 12 \\ 18 & 23 \end{bmatrix}\begin{bmatrix} 9 \\ 7 \end{bmatrix} = \begin{bmatrix} 291 \\ 323 \end{bmatrix} \bmod 29 \equiv \begin{bmatrix} 1 \\ 4 \end{bmatrix}$$

Dengan cara yang sama dengan cara pada proses enkripsi, menggunakan $P_{1,2}$ didapatkan:

$$i = 1$$
$$n = 2$$
$$Z = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

Lakukan D_K2 terhadap blok plainteks berikutnya diikuti proses D_K1 dengan rumus:

$$P_{3,4} = D_K1(D_K2(C_{3,4}))$$
$$= D_K1(C_{3,4} - (i.Z))$$
$$= D_K1\left(\begin{bmatrix} 19 \\ 11 \end{bmatrix} - 1\begin{bmatrix} 2 \\ 1 \end{bmatrix}\right)$$
$$= D_K1\left(\begin{bmatrix} 17 \\ 10 \end{bmatrix}\right)$$
$$= K^{-1}.\begin{bmatrix} 17 \\ 10 \end{bmatrix}$$
$$= \left(\begin{bmatrix} 23 & 12 \\ 18 & 23 \end{bmatrix}\begin{bmatrix} 17 \\ 10 \end{bmatrix}\right) \bmod 29$$
$$\equiv \begin{bmatrix} 18 \\ 14 \end{bmatrix}$$

Hitung n dan Z untuk blok-blok berikutnya dan ulangi langkah diatas hingga blok habis.

Hasil dekripsi cipherteks C menghasilkan plainteks:

P = 1 4 18 14 10 26 12 0 11 0 12 27

P = B E S O K M A L A M .

4.4. Analisis terhadap *chaining hill cipher*

Hasil analisis terhadap *chaining hill cipher* adalah:

Chaining hill cipher dapat mengurangi kemungkinan penggunaan *brute force* dalam pemecahannya karena penggunaan 29 karakter menambah kemungkinan kunci yang ada menjadi lebih dari 2 kali lipat dibanding penggunaan 26 karakter. Hal ini disebabkan, pada Z_{26}, matriks yang memiliki nilai determinan genap, 0 dan 13 tidak memiliki *multiplicative inverse*, sementara pada Z_{29}, hanya matriks dengan determinan 0 yang tidak memiliki *multiplicative inverse.*

Chaining hill cipher masih dapat dipecahkan dengan menggunakan *known-plaintext attack* dengan menggunakan persamaan linier. Namun proses pemecahan jauh lebih rumit dibanding *hill cipher* biasa dan kriptanalis membutuhkan informasi tambahan mengenai proses enkripsi yang dilakukan untuk dapat memecahkannya.

5. KESIMPULAN

Berdasarkan pembahasan yang telah dilakukan diatas, maka kesimpulan yang dapat diambil adalah:

1. *Hill cipher* adalah algoritma kriptografi klasik yang sangat kuat dilihat dari segi keamanannya.
2. Matriks kunci *hill cipher* harus merupakan matriks yang *invertible*.
3. *Hill cipher* kuat dalam menghadapi *ciphertext-only attack* namun lemah jika diserang dengan *known-plaintext attack.*
4. Teknik kriptanalisis menggunakan persamaan linier merupakan teknik yang paling cepat, mudah dan akurat untuk memecahkan *hill cipher* dibanding dengan teknik perkalian matriks.
5. Modifikasi yang dilakukan penulis terhadap *hill cipher* menjadi *chaining hill cipher* cukup efektif menambah kekuatan algoritma kriptografi klasik ini dengan penggunaan 29 karakter dan proses enkripsi yang lebih rumit.
6. Komputasi dalam *hill cipher* cukup rumit jika dihitung secara manual untuk teks yang panjang. Penulis membuat dan menggunakan program[1] untuk melakukan pengujian pada *hill cipher* dan *chaining hill cipher* dengan teks yang panjang.
7. *Chaining hill cipher* ternyata masih dapat dipecahkan dengan *known-plaintext attack.* Namun perubahan yang diberikan membuat proses kriptanalisis menjadi lebih sulit dan membutuhkan perkiraan, sehingga memakan waktu lebih lama.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, 2006.

[2] Forouzan, Behrouz, *Cryptography and Network Security*, McGraw-Hill, 2008.

[3] http://en.wikipedia.org/wiki/Hill_cipher

[4] www.cs.iupui.edu/~xkzou/teaching/csci590/chapter1_l2.ppt

[5] H. Anton, C. Rorres, *Elementary Linear Algebra*, John Wiley & Sons, 2000.

[1] Implementasi sederhana untuk kunci berukuran 2×2. Dapat di-*download* di http://students.if.itb.ac.id/~if14030/chc.zip