**Algoritma Hill Cipher (Sandi Hill)**

[22 Maret 2015](https://muamalkhoerudin.wordpress.com/2015/03/22/algoritma-hill-cipher-sandi-hill/) [muamalkhoerdin](https://muamalkhoerudin.wordpress.com/author/muamalkhoerdin/)

***Hill Cipher***merupakan salah satu algoritma kriptografi kunci simetris yang memiliki beberapa kelebihan dalam enkripsi data. Untuk menghindari matrik kunci yang tidak *invertible*, matrik kunci dibangkitkan menggunakan koefisien binomial newton.  Proses enkripsi dan deskripsi menggunakan kunci yang sama, plaintext dapat menggunakan media gambar atau text.

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.

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

Hill Cipher yang merupakan polyalphabetic cipher dapat dikategorikan sebagai block cipher [2] karena teks yang akan diproses akan dibagi menjadi blokblok 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.

Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas ciphertext saja. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas ciphertext dan potongan berkas plaintext. Teknik kriptanalisis ini disebut known-plaintext attack [1].

**Dasar Teknik Hill Cipher**

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. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki inverse K-1 sehingga :

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

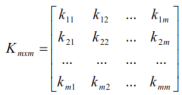
**Algoritma Enkripsi Hill Cipher**

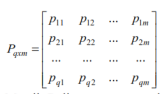
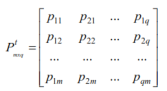
 Tahapan-tahapan algoritma enkripsi Hill Cipher sebagai berikut :

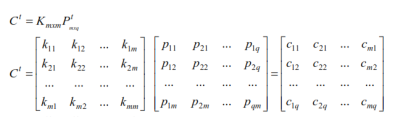
1. Korespondenkan abjad dengan numerik

*A* → 1, *B* → 2,…, *Z* → 26

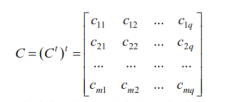
1. Buat matriks kunci berukuran m x m

[](https://muamalkhoerudin.files.wordpress.com/2015/03/a.png)

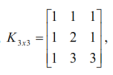
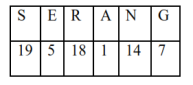
1. Matrik  K  merupakan  matriks  *yang  invertible*yaitu  memiliki  *multiplicative inverse  K* −1 sehingga  *K*.*K* −1  = 1
2. Plainteks *P* = *p*1 *p*2 … *pn* ,   diblok dengan ukuran sama dengan  baris atau kolom matrik K, sehingga [](https://muamalkhoerudin.files.wordpress.com/2015/03/b.png)
3. Matrik P di transpose menjadi[](https://muamalkhoerudin.files.wordpress.com/2015/03/c.png)
4. Kalikan Matrik K dengan Matrik P transpose dalam modulo 26

[](https://muamalkhoerudin.files.wordpress.com/2015/03/d.png)

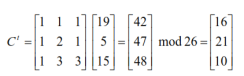
1. Kemudian ditransposekan

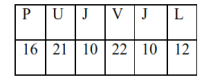
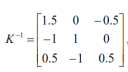
[](https://muamalkhoerudin.files.wordpress.com/2015/03/e.png)

1. Ubah hasil langkah ke-7 kedalam abjad menggunakan koresponden abjad dengan numerik pada langkah 1 sehingga diperoleh cipherteks

**Proses Enkripsi** Untuk membahas proses enkripsi dan dekripsi dipilih contoh plaintext “**SERANG**”. Matrik kunci yang diperoleh dari koefisien binomial ukuran 3 x 3 [](https://muamalkhoerudin.files.wordpress.com/2015/03/g.png) Koresponden plaintext dengan tabel abjad [](https://muamalkhoerudin.files.wordpress.com/2015/03/f.png)

Didapat  bilangan  desimal  dalam  Z26   untuk  plainteks  SERANG  yaitu  19,5,18,1,14,7 sehingga  diperoleh   plainteks *P* = [19 5   18 1  14 7] .Karena   matrik   kunci berukuran 3×3 maka matriks plainteks yang diambil adalah *P* = [19  5  15], matriks P di transpose menjadi [h](https://muamalkhoerudin.files.wordpress.com/2015/03/h.png)Kemudian matriks kunci dikalikan dengan matriks P yang sudah ditranspose

[](https://muamalkhoerudin.files.wordpress.com/2015/03/i.png)

*C* = (*C t* )*t*= [16  21  10], korespondensikan matrik C dengan tabel abjad dengan **“PUJ”**, dengan   cara   yang   sama   untuk   plainteks *P* = [1   14   7] ,   diperoleh   cipherteks *C* = (*C t* )*t*= [22   10  12] dan dikorespondenkan diperoleh  **“VJL”** , sehingga cipherteks dari plainteks “**SERANG**” adalah “**PUJVJL**” **Proses Dekripsi** Cipherteks yang sudah diperoleh akan di dekripsi sehingga akan menjadi kata yang mempunyai makna. Cipherteks “**PUJVJL**” dikoresponden dengan tabel abjad  menjadi [](https://muamalkhoerudin.files.wordpress.com/2015/03/j.png)Sehingga cipherteks menjadi *C* = [16   21  10   22  10 12], karena ukuran matriks kunci 3×3 sehingga cipherteks dibagi menjadi 2 yaitu *C* = [16   21  10] dan *C* = [22   10   12]. Invers dari Matriks Kunci  [](https://muamalkhoerudin.files.wordpress.com/2015/03/k.png)

kalikan matriks *K*dengan matriks [n](https://muamalkhoerudin.files.wordpress.com/2015/03/n.png) selanjutnya matriks di transpose menjadi [o](https://muamalkhoerudin.files.wordpress.com/2015/03/o.png)

Dengan cara yang sama dengan mengambil  *C* = [22    10  12] diperoleh matriks  *P* = (*Pt* )*t*= [1   14  7] dengan mengabungkan kedua plainteks maka nilai *P* = [19   5   18  1  14  7]dan jika dikorespondesikan dengan tabel abjad menjadi “**SERANG**” sama dengan plainteks awal.

**Algoritma Deskripsi Hill Cipher**

1. Korespondekan abjad dengan numerik

*A* → 1, *B* → 2,…, *Z* → 26

1. Ubah cipherteks kedalam numerik
2. Kunci yang digunakan untuk mendekrip ciphertext ke plaintext adalah invers dari matrik kunci *K mxm*
3. Menghitung  *K* −1
4. Kalikan  invers  matriks  kunci  dengan  cipherteks  transpose  dalam  modulo  26, diperoleh plainteks transpose  *P t*= *K* −1*C t*
5. Dari langkah ke-5 diperoleh  *P* = (*P t* ) *t*
6. Korespondensikan abjad dengan numerik hasil langkah 6 diperoleh plainteks

**Teknik Enkripsi pada Hill Cipher**

Proses enkripsi pada Hill Cipher dilakukan per blok plaintext. Ukuran blok tersebut sama dengan ukuran matriks kunci. Sebelum membagi teks menjadi deretan blok-blok, plaintext terlebih dahulu dikonversi menjadi angka, masing-masing sehingga A=1, B=2, hingga Y=25. Z diberi nilai 0.

[](https://muamalkhoerudin.files.wordpress.com/2015/03/1.jpg)

 Secara matematis, proses enkripsi pada Hill Cipher adalah:

*C = K . P (2)*

*C = Ciphertext*

*K = Kunci*

*P = Plaintext*

 Jika terdapat plaintext P:

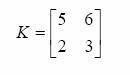
 P = STRIKE NOW

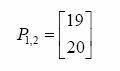
 Maka plaintext tersebut dikonversi menjadi:

 P = 19 20 18 9 11 5 14 15 23

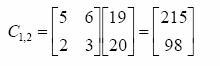
 Plaintext tersebut akan dienkripsi dengan teknik Hill

*Cipher*, dengan kunci K yang merupakan matriks 2×2.

[](https://ciiekaajn.files.wordpress.com/2011/03/picture13.jpg)Karena matriks kunci K berukuran 2, maka *plaintext* dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter. Karena karakter terakhir tidak ada memiliki pasangan, maka diberi pasangan karakter yang sama yaitu W. P menjadi STRIKENOWW. Blok pertama dari *plaintext* P adalah :

[](https://ciiekaajn.files.wordpress.com/2011/03/picture14.jpg)

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

[](https://ciiekaajn.files.wordpress.com/2011/03/picture15.jpg)

Hasil perhitungan menghasilkan angka yang tidak berkorespondensi dengan huruf-huruf, maka lakukan modulo 26 pada hasil tersebut. Sehingga, C1,2 menjadi:

[https://ciiekaajn.files.wordpress.com/2011/03/picture17.jpg?w=614](https://ciiekaajn.files.wordpress.com/2011/03/picture17.jpg)

Karakter yang berkorespondensi dengan 7 dan 20 adalah G dan T. maka S menjadi G dan T menjadi T. Setelah melakukan enkripsi semua blok pada *plaintext* P maka dihasilkan *ciphertext* C sebagai berikut:

P = STRIKENOW

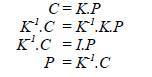
C = 7 20 14 11 7 11 4 21 19 11

C = GTNKGKDUSK

Dari *ciphertext* yang dihasilkan terlihat bahwa *Hill Cipher* menghasilkan *ciphertext* yang tidak memiliki pola yang mirip dengan *plaintext*nya.

Teknik Dekripsi pada *Hill Cipher*

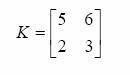
Proses dekripsi pada *Hill Cipher* pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (invers) terlebih dahulu. Secara matematis, proses dekripsi pada *Hill Cipher* dapat diturunkan dari persamaan (2).

[](https://ciiekaajn.files.wordpress.com/2011/03/picture20.jpg)

Menjadi persamaan proses dekripsi:

[https://ciiekaajn.files.wordpress.com/2011/03/picture21.jpg?w=614](https://ciiekaajn.files.wordpress.com/2011/03/picture21.jpg)

Dengan menggunakan kunci

[](https://ciiekaajn.files.wordpress.com/2011/03/picture13.jpg), maka proses dekripsi diawali dengan mencari invers dari matriks *K.* Mencari invers dapat dilakukan dengan menggunakan metode operasi baris (row operation) atau metode determinan [3]. Setelah melakukan perhitungan, didapat matriks *K-1* yang merupakan invers dari matriks *K*, yaitu :

[https://ciiekaajn.files.wordpress.com/2011/03/picture121.jpg?w=614](https://ciiekaajn.files.wordpress.com/2011/03/picture121.jpg)

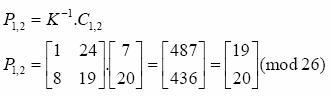
Kunci K-1 yang digunakan untuk melakukan dekripsi ini telah memenuhi persamaan (1) karena:

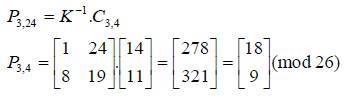
[https://ciiekaajn.files.wordpress.com/2011/03/picture16.jpg?w=614](https://ciiekaajn.files.wordpress.com/2011/03/picture16.jpg)

*Ciphertext* C = GTNKGKDUSK, 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 *ciphertext*menjadi urutan numerik.

C = 7 20 14 11 7 11 4 21 19 11

Proses dekripsi dilakukan sebagai berikut:

[](https://ciiekaajn.files.wordpress.com/2011/03/picture111.jpg)dan blok kedua:

[](https://ciiekaajn.files.wordpress.com/2011/03/picture22.jpg)

Setelah semua blok selesai didekripsi, maka didapatkan hasil *plaintext*:

P = 19 20 18 9 11 5 14 15 23

P = STRIKENOW

**Hill cipher**

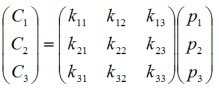
1. Dikembangkan oleh Lester Hill (1929)
2. Menggunakan m buah persamaan linier
3. Untuk m = 3 (enkripsi setiap 3 huruf),

  C1 = (k11 p1 + k12p2 + k13 p3) mod 26

  C2 = (k21 p1 + k22p2 + k23 p3) mod 26

  C3 = (k31 p1 + k32p2 + k33 p3) mod 26

atau:

[](https://muamalkhoerudin.files.wordpress.com/2015/03/2.png)

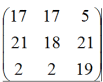
atau **C** = **KP**

 Dekripsi perlu menghitung **K**-1sedemikian sehingga

**KK**-1= **I**   (**I** matriks identitas).

 Contoh:

**K =**

[](https://muamalkhoerudin.files.wordpress.com/2015/03/3.png)

 Plainteks: PAYMOREMONEY

 Enkripsi tiga huruf pertama: PAY = (15, 0, 24)

 Cipherteks: C =

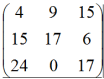
[4](https://muamalkhoerudin.files.wordpress.com/2015/03/4.png)

                        = **LNS**

 Cipherteks selengkapnya: **LNSHDLEWMTRW**

 Dekripsi,

**K**-1=

[](https://muamalkhoerudin.files.wordpress.com/2015/03/5.png)

 sebab

[6](https://muamalkhoerudin.files.wordpress.com/2015/03/6.png)

 Dekripsi:

**P** = **K**-1 **C**

Cipherteks: LNS  atau C = (11, 13, 18)

  Plainteks:

[7](https://muamalkhoerudin.files.wordpress.com/2015/03/7.png)

**C** = (15, 0, 24) = (P, A, Y)

Kekuatan Hill cipher terletak pada penyembunyian frekuensi huruf tunggal

Huruf plainteks yang sama belum tentu dienkripsi menjadi huruf cipherteks yangsama.

Hill cipher mudah dipecahkan dengan known-plaintext attack.

Misalkan untuk Hill cipher dengan m = 2 diketahui:

–P = (5, 17) dan C = (15, 16)

–P = (8, 3) dan C = (2, 5)

–Jadi, **K**(5, 17) = (15, 16) dan **K**(8, 3) = (10, 20)

[8](https://muamalkhoerudin.files.wordpress.com/2015/03/8.png)

Inversi dari X adalah

[9](https://muamalkhoerudin.files.wordpress.com/2015/03/9.png)

 Sehingga

[10](https://muamalkhoerudin.files.wordpress.com/2015/03/10.png)

**Kesimpulan** Berdasarkan pembahasan diatas kesimpulan yang dapat diambil adalah :

1. Koefisien binomial dapat dijadikan sebagai matrik kunci
2. Matriks kunci *hill cipher* harus matriks yang *invertible*
3. Setiap pesan yang dienkripsi harus mempunyai panjang kelipatan dari n yaitu banyaknya kolom pada matriks kunci.
4. Hasil enkripsi plainteks yang sama dengan menggunakan matriks kunci yang berbeda akan menghasilkan cipherteks yang berbeda.

**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 *ciphertext 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 *knownplaintext attack*. Jika kriptanalisis memiliki pecahan *plaintext* dan *ciphertext* yang saling berkorespondensi, maka *Hill Cipher* dapat dipecahkan. Namun proses yang cukup sulit adalah untuk menentukan panjang kunci yang digunakan.

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.

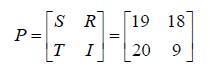
Kemungkinan terburuk yang dimiliki oleh *Hill Cipher* adalah ketika seorang kriptanalis memiliki potongan *plaintext* dan*ciphertext* yang berkorespondensi serta mengetahui panjang kunci yang digunakan. Dengan informasi ini, kriptanalis dapat memecahkan *Hill Cipher* dengan sangat mudah. Misalkan kriptanalis mengetahui panjang kunci K adalah 2 dan memiliki potongan berkas *plaintext* P dan C sebagai berikut:

P = STRI

C = GTNKGKDUSK

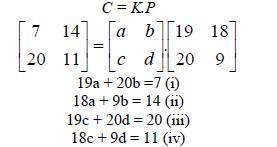
Dari informasi yang dimiliki, maka diketahui bahwa karakter ST pada *plaintext* berkorespondensi dengan karakter GT, dan karakter RI dengan NK. Pemecahan dapat dilakukan dengan persamaan linier Misalkan kunci direpresentasikan dengan:

[https://ciiekaajn.files.wordpress.com/2011/03/picture23.jpg?w=614](https://ciiekaajn.files.wordpress.com/2011/03/picture23.jpg)Plaintext P dengan:

[](https://ciiekaajn.files.wordpress.com/2011/03/picture24.jpg)Ciphertext C dengan:

[https://ciiekaajn.files.wordpress.com/2011/03/picture25.jpg?w=614](https://ciiekaajn.files.wordpress.com/2011/03/picture25.jpg)

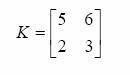
Dengan menerapkan persamaan (2) maka persamaan linier yang dapat dibentuk dari contoh adalah:

[](https://ciiekaajn.files.wordpress.com/2011/03/picture26.jpg)

Dengan menyelesaikan persamaan (i) dan persamaan (ii) lalu persamaan (iii) dan persamaan (iv) memakai aritmatika modulo 26, maka nilai a, b, c, dan d didapat:

a = 5  
b = 6  
c = 2  
d = 3

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

[](https://ciiekaajn.files.wordpress.com/2011/03/picture13.jpg)Dengan kunci K tersebut, kriptanalis hanya perlu melakukan dekripsi terhadap ciphertext keseluruhan untuk mendapatkan plaintext seutuhnya.  
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. Semakin besar suatu matriks kunci maka semakin kuat juga segi keamanannya.
3. Hill Cipher kuat dalam menghadapi ciphertext-only attack namun lemah jika diserang dengan knownplaintext attack.