Nama : Meira Dwiana Anjani
Anne Audistya F
NPM : 140810180015
140810180059
Kelas : A

Hill Cipher

Hill Cipher merupakan salah satu algoritma kriptografi yang memanfaatkan kunci berupa matriks untuk melakukan enkripsi dan dekripsi selain itu juga menggunakan aritmatika modulo.

Syarat Matriks Kunci

1. Determinan tidak sama dengan nol
2. Matriks berupa persegi atau jumlah baris dan kolom sama
3. Jumlah dan kolomnya merupakan bilangan prima terkecil yang menjadi faktor dari jumlah karakter yang akan di enkripsi

- Algoritma Enkripsi Hill Cipher
  1. Tentukan Plaintext
  2. Susun plaintext dalam bentuk blok matriks (2x1 jika kunci ber-ordo 2x2, 3x1 jika kunci berordo 3x3)
  3. Tentukan matriks kunci (nilai determinan harus ganjil positif atau negatif)
  4. Lakukan proses dengan rumus

$$C = mP * mK$$

Ket :

C = Ciphertext

mK = Matriks Kunci

mP = Matriks Plaintext

Contoh :

Enkripsikan GOPHER dengan kunci $K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$

Maka langkah yang dapat kita lakukan adalah :

1. Tuliskan urutan huruf dari plaintext “GOPHER”

G	O	P	H	E	R
6	14	15	7	4	17

2. Susun plaintext ke dalam bentuk blok matriks. Karena matriks kunci berordo 2x2, maka bentuk matriksnya adalah 2x1.

G	O	P	H	E	R
6	14	15	7	4	17
Matriks 1		Matriks 2		Matriks 3	

3. Kalikan matriks plaintext dengan matriks kunci
   a. GO

      $C = [6 \quad 14] \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} \bmod 26 = [4 \quad 16] = [E \quad Q]$

   b. PH

      $C = [15 \quad 7] \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} \bmod 26 = [4 \quad 13] = [E \quad N]$

   c. ER

      $C = [4 \quad 17] \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} \bmod 26 = [17 \quad 21] = [R \quad V]$

   Sehingga didapatkan hasil enkripsi :

   E Q E N R V

- Algoritma Dekripsi Hill Cipher

Proses dekripsi pada Hill Cipher pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (invers) terlebih dahulu.

Tahapan :

1. Menentukan matriks Chipertext (Ct)
2. Tentukan determinan matriks kunci K

$$|K| = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - cd$$

3. Tentukan nilai invers modulo
4. Tentukan invers matriks kunci K
5. Tentukan kunci dekripsi Hill Cipher K^{-1}
6. Rumus dekripsi Hill Cipher

$$P = mK^{-1} * mC$$

Ket :

P = Plaintext

mK^{-1} = Invers Matriks Kunci

mC = Matriks Ciphertext

Contoh :

Dekripsikan SLHYAT dengan kunci $K = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$

Maka langkah yang dapat kita lakukan adalah :

1. Tuliskan urutan huruf dari plaintext “SLHYAT” dan urutkan ke dalam blok matriks

S	L	H	Y	A	T
18	11	7	24	0	19
Matriks 1		Matriks 2		Matriks 3	

2. Menentukan determinan matriks K :

$\begin{vmatrix} 2 & 1 \\ 3 & 4 \end{vmatrix}$ = (2 x 4) – (3 x 1) = 5

3. Menentukan invers modulo :

5^{-1} mod 26 → gcd (5, 26) = 1.

$26 = 5(5) + 1$

$5 = 5(1) + 0$

Invers modulo $5^{-1}\ mod\ 26 = 21$

4. Tentukan invers matriks kunci K

$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}^{-1} = \frac{1}{(2\ x\ 4) - (3\ x\ 1)} \begin{bmatrix} 4 & -1 \\ -3 & 2 \end{bmatrix}$

5. Menentukan matriks K baru hill cipher

$$21 \begin{bmatrix} 4 & -1 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 84 & -21 \\ -63 & 42 \end{bmatrix} mod\ 26 = \begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix}$$

6. Melakukan proses dekripsi Hill Cipher

$$(18 \quad 11) \begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix} = [\ 163 \quad 446\ ] mod\ 26 = [\ 7 \quad 4]$$

$$(7 \quad 25) \begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix} = [\ 167 \quad 505] mod\ 26 = [\ 11 \quad 11]$$

$$(24 \quad 0) \begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix} = [\ 114 \quad 360] mod\ 26 = [\ 14 \quad 22]$$

Sehingga dapat dihasilkan hasil dekripsi : H E L L O W

- Mencari Kunci Hill Cipher

  Sebagai contoh :

  PT : FRIDAY ; CT : PQCFKU ; m = 2

  Dit. key dari hill cipher?

  Maka tahapan yang dapat kita lakukan adalah :

1. Menulis urutan huruf alphabet satu persatu (baik plaintext maupun cipher text)

   FRIDAY → (5, 17, 8, 3, 0, 24);

   PQCFKU → (15, 16, 2, 5, 10, 20)

2. Setelah melihat urutan seperti diatas, maka dapat disimpulkan bahwa,

   Hasil enkripsi :

   e_k (5,17) = (15,16);

   e_k (8, 3) = (2, 5);

   e_k (0,24) = (10,20)

3. Ubah rumus enkripsi ke dalam bentuk matriks. Karena m = 2, maka ambil 2 enkripsi (4 huruf).

$$\begin{bmatrix} 15 & 16 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 5 & 17 \\ 8 & 3 \end{bmatrix} K$$

4. Jika

$$P = mK^{-1} * mC$$

   Maka

$$mK = mC^{-1} * mP$$

5. Bentuk ke matriks rumus tersebut

$$K = \begin{bmatrix} 5 & 17 \\ 8 & 13 \end{bmatrix}^{-1} \begin{bmatrix} 15 & 16 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 137 & 149 \\ 60 & 107 \end{bmatrix} mod\ 26 = \begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$$

Maka didapat matriks kunci K =

$$\begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$$