**DASAR TEKNIK HILL CIPHER**

Hill chiper merupakan salah satu algoritma kriptografi kunci simetris. Algoritma Hill Cipher menggunakan matriks berukuran mxn 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. Dasar Teknik Hill Cipher adalah aritmatika modulo terhadap matriks. Dalam penerapannya, Metode Hill Cipher menggunakan teknik perkalian matriks dan invers terhadap matriks. Matriks yang digunakan pada Hill cipher adalah matriks yang *invertible.* Matriks i*nvertible* adalah matriks yang berukuran n x n dan memiliki determinan ≠ 0 sehingga memiliki invers.

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

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

Tabel 1. Konversi Alfabet ke angka

**PROSES HILL CIPHER MATRIKS**

1. **Enkripsi**

Secara matematis, proses enkripsi pada hill *Cipher* adalah : *C = K . P*

* *C* = *Ciphertext*
* *K* = Kunci
* *P* = *Plaintext*
* Jika terdapat *plaintext* P: P = STRIKE NOW
  + Maka *plaintext* tersebut dikonversi menjadi:
  + P = ……………………… ??
* *Plaintext* tersebut akan dienkripsi dengan teknik *Hill Cipher*, dengan kunci K yang merupakan matriks 2×2.

Blok pertama dari *plaintext* P adalah

* Blok *plaintext* ini kemudian dienkripsi dengan kunci K melalui persamaan
* Hasil perhitungan menghasilkan angka yang tidak berkores pondensi dengan huruf-huruf, maka lakukan modulo26 pada hasil tersebut. Sehingga, C1,2 menjadi:
* 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 = STRIKE NOW

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

C = GTNKGKDUSK

1. **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 *HillCipher* dapat diturunkan dari persamaan (2).
* Menjadi persamaan proses dekripsi:
* Dengan menggunakan kunci :
* Maka proses dekripsi diawali dengan mencari invers dari matriks *K.*
* Mencari invers dapat dilakukan dengan menggunakan metode operasi baris (row operation) atau metode determinan.
* Setelah melakukan perhitungan, didapat matriks

*K*-1 yang merupakan invers dari matriks *K*, yaitu :

K-1 = ……… ???

K.K-1 = ……… ???

* Hasil :
* *Ciphertext* C = GTNKGKDUSK, akan didekripsi dengan menggunakan kunci dekripsi K-1 dengan persamaan.
* 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 blok pertama : …. ???
* Blok kedua :
* Setelah semua blok selesai didekripsi, maka didapatkan hasil *plaintext*:

P = 18 19 17 8 10 4 13 14 22

P = STRIKENOW