**DASAR TEKNIK HILL CIPHER**

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. Jika matriks kunci memiliki determinan = 26, maka matriks dapat digunakan dalam proses enkripsi, namun akan gagal ketika proses deskripsi. Sehingga menjadi penting untuk diperhatikan dalam memilih matriks kunci yang sesuai.

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 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 |

Tabel 1. Konversi Alfabet ke angka

**PROSES HILL CIPHER MATRIKS**

1. **Enkripsi**

Secara sistematis, proses enkripsi pada Hill Cipher adalah :

= . (4.1)

C = *Ciphertext*.

K = *Kunci*

P = *Plaintext.*

Kasus : terdapat plaintext P = JEPARA, dan kunci maka :

1. Bagi *Plaintext* P menjadi matriks 2 x 1 dan konversi menjadi angka sesuai table

=

=

=

1. Kalikan setiap angka dengan matriks kunci

K =

= =

= =

= =

1. Lakukan operasi Mod 26 kepada setiap matriks angka tersebut agar dapat dikonversi menggunakan table.1

Mod 26 =

Mod 26 =

Mod 26 =

1. Ubah setiap matriks angka menjadi huruf dengan aturan konversi seperti table.1

=

=

=

1. Pesan JEPARA dienkripsi menjadi YXGZKF
2. **Deskripsi**

Sama dengan proses enkripsi tetapi matriks kunci harus dibalik (invers) terlebih dahulu. Secara matemati proses deskripsi di turunkan dari persamaan 4.1

= .

-1. = -1 . .

-1 . = .

= -1 .

Proses deskripsi dapat ditulis dengan persamaan :

= -1 . (4.2)

P = *Plaintext.*

K-1 = Invers matriks

Kunci. C = *ciphertext.*

K-1 = invers matriks kunci.

Invers matriks dapat dicari menggunaka operasi baris elementer (OBE) atau prinsip detereminan.

K-1 =

K-1 = Mod 26

K-1 =

1. Bagi *plaintext* P menjadi matriks 2 x 1 dan konversi menjadi angka sesuai table.1

=

=

=

1. Kalikan setiap angka dengan matriks kunci
2. Lakukan operasi mod 26 kepada setiap matriks angka tersebut agar dapat dikonversi dengan table.1

Mod 26 =

Mod 26 =

Mod 26 =

1. Ubah setiap matriks angka menjadi huruf dengan aturan konversi seperti table.1

=

=

=

1. Didapatkan pesan YXGZKF yang telah dideskripsi menjadi : JEPARA

