KRIPTOGRAFI – PERTEMUAN 5

HILL CIPHER

Sindhu Rakasiwi, M.Kom
sindhu.rakasiwi@dsn.dinus.ac.id

Hill Cipher

- Hill cipher merupakan salah satu teknik penyandian yang menggunakan kunci simetris, yaitu kunci yang sama – sama digunakan dalam proses enkripsi maupun dekripsi. Hill cipher diusulkan oleh Lester S. Hill pada tahun 1929. Tujuan dari dibentuknya teknik ini adalah untuk menciptakan teknik penyandian yang tidak dapat dipecahkan menggunakan analisa frekuensi. Hill cipher memanfaatkan operasi matriks yaitu perkalian dan *inverse* matriks.
- Kunci yang digunakan pada Hill cipher berupa matriks berukuran $m \times m$ yang akan dipakai dalam proses enkripsi maupun dekripsi. Selain itu, Hill cipher juga memanfaatkan operasi modulo 26 untuk membentuk *ciphertext* ataupun mengembalikan *plaintext*. Digunakannya modulo 26 karena huruf – huruf alfabet yang berjumlah 26 akan disusun sebagai berikut:

Hill Cipher

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

- Tiap huruf dalam alfabet akan diberi indeks angka dimulai dari huruf ‘A’ yang berindeks 0 (nol). Untuk dapat melakukan enkripsi, matriks kunci *m*×*m* yang digunakan harus memiliki syarat yaitu:
  - Matriks kunci harus *invertible* atau dapat di-*inverse*-kan sehingga memenuhi persamaan matriks:
  - $K.\ K^{-1} = I$
  - Nilai determinan dari matriks kunci tersebut harus bilangan coprima (*relative prime*) terhadap 26.

Hill Cipher

- Kemudian untuk dapat melakukan proses enkripsi dan dekripsi gunakan persamaan dibawah ini
- Enkripsi

$$C = E(K,C) = KP \bmod 26$$

- Dekripsi

$$P = D(K,P) = K^{-1}C \bmod 26$$

Studi Kasus

- *Plaintext* "EKO HARI" akan dienkripsi menggunakan kunci matriks dibawah ini:

$$\text{Matriks kunci} = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$$

- Langkah pertama adalah susun *plaintext* menjadi matriks berukuran 2×1 karena ukuran matriks kunci adalah 2×2 maka nilai *m* = 2.

$$\begin{bmatrix} E \\ K \end{bmatrix} = \begin{bmatrix} 4 \\ 10 \end{bmatrix}$$
$$\begin{bmatrix} O \\ H \end{bmatrix} = \begin{bmatrix} 14 \\ 7 \end{bmatrix}$$
$$\begin{bmatrix} A \\ R \end{bmatrix} = \begin{bmatrix} 0 \\ 17 \end{bmatrix}$$
$$\begin{bmatrix} I \\ X \end{bmatrix} = \begin{bmatrix} 8 \\ 23 \end{bmatrix}$$

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Studi Kasus

- Dikarenakan nilai terakhir tidak memiliki pasangan matriks maka sisipkan huruf ‘X’ sebagai pasangan pelengkap. Kemudian lakukan perkalian matriks antara matriks kunci dengan matriks *plaintext*.

$$\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}\begin{bmatrix} 4 \\ 10 \end{bmatrix} = \begin{bmatrix} (5 \times 4) + (8 \times 10) \\ (17 \times 4) + (3 \times 10) \end{bmatrix} = \begin{bmatrix} 100 \\ 98 \end{bmatrix} mod\ 26 = \begin{bmatrix} 22 \\ 20 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}\begin{bmatrix} 14 \\ 7 \end{bmatrix} = \begin{bmatrix} (5 \times 14) + (8 \times 7) \\ (17 \times 14) + (3 \times 7) \end{bmatrix} = \begin{bmatrix} 126 \\ 259 \end{bmatrix} mod\ 26 = \begin{bmatrix} 22 \\ 25 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}\begin{bmatrix} 0 \\ 17 \end{bmatrix} = \begin{bmatrix} (5 \times 0) + (8 \times 17) \\ (17 \times 0) + (3 \times 17) \end{bmatrix} = \begin{bmatrix} 136 \\ 51 \end{bmatrix} mod\ 26 = \begin{bmatrix} 6 \\ 25 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}\begin{bmatrix} 8 \\ 23 \end{bmatrix} = \begin{bmatrix} (5 \times 8) + (8 \times 23) \\ (17 \times 8) + (3 \times 23) \end{bmatrix} = \begin{bmatrix} 224 \\ 205 \end{bmatrix} mod\ 26 = \begin{bmatrix} 16 \\ 23 \end{bmatrix}$$

Studi Kasus

- Dari perhitungan diatas didapatkan matriks cipher baru dengan melakukan operasi modulo 26 pada hasil perkalian matriks. Kemudian matriks cipher baru tersebut dikonversikan menjadi karakter *ciphertext* baru menggunakan tabel indeks diatas. Sehingga hasil dari proses enkripsi Hill cipher adalah:

$$\begin{bmatrix}22\\20\end{bmatrix} = \begin{bmatrix}W\\U\end{bmatrix}$$
$$\begin{bmatrix}22\\25\end{bmatrix} = \begin{bmatrix}W\\Z\end{bmatrix}$$
$$\begin{bmatrix}6\\25\end{bmatrix} = \begin{bmatrix}G\\Z\end{bmatrix}$$
$$\begin{bmatrix}16\\23\end{bmatrix} = \begin{bmatrix}Q\\X\end{bmatrix}$$

Hasil enkripsi = “WUWZGZQX”

Studi Kasus

- Sementara itu untuk melakukan dekripsi pada Hill cipher dengan hasil enkripsi (*ciphertext*) = “WUWZGZQX”, proses pertama adalah menginvertkan matriks kunci. Untuk menginvertkan matriks kunci, tentukan terlebih dahulu nilai determinan dari matriks kunci tersebut.
- Matriks kunci = $\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$
- Determinan = ad - bc
- Determinan = (5 × 3) – (8 × 17) = –121
- Setelah nilai determinan ditemukan, aplikasikan operasi modulo 26 pada hasil determinan tersebut. sehingga:
- –121 *mod* 26 = 9
- Selanjutnya, mencari K^{-1} dari matriks kunci yang juga dioperasikan dengan modulo 26.
- $K^{-1} = \frac{1}{\det K}\begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} = 9^{-1} \, mod \, 26 \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix}$

Studi Kasus

- Untuk mencari nilai 9^{-1} *mod* 26 gunakan perhitungan modular inverse dimana memenuhi persamaan (9×*M*) *mod* 26 = 1. Sehingga didapatkan nilai modular inverse (*M*) dari 9^{-1} *mod* 26 adalah 3 karena nilai tersebut memenuhi (9×3) *mod* 26 = 27 *mod* 26 = 1.

$$\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$$

- Sehingga untuk membentuk nilai K^{-1} maka:

$$9^{-1}\ mod\ 26 \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} = 3 \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} mod\ 26$$
$$= \begin{bmatrix} 3 \times 3 & -8 \times 3 \\ -17 \times 3 & 5 \times 3 \end{bmatrix} mod\ 26$$
$$= \begin{bmatrix} 9 & -24 \\ -51 & 15 \end{bmatrix} mod\ 26$$
$$K^{-1} = \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix}$$

- Gunakan nilai K^{-1} untuk mendekripsikan *ciphertext* dengan melakukan operasi perkalian matriks. Terlebih dahulu susun *ciphertext* menjadi matriks 2×1.

$$\begin{bmatrix} 22 \\ 20 \end{bmatrix} = \begin{bmatrix} W \\ U \end{bmatrix}$$
$$\begin{bmatrix} 22 \\ 25 \end{bmatrix} = \begin{bmatrix} W \\ Z \end{bmatrix}$$
$$\begin{bmatrix} 6 \\ 25 \end{bmatrix} = \begin{bmatrix} G \\ Z \end{bmatrix}$$
$$\begin{bmatrix} 16 \\ 23 \end{bmatrix} = \begin{bmatrix} Q \\ X \end{bmatrix}$$

Studi Kasus

- Kemudian kalikan matriks cipher dengan kunci K^{-1}

$$\begin{bmatrix}9 & 2\\ 1 & 15\end{bmatrix}\begin{bmatrix}22\\ 20\end{bmatrix} = \begin{bmatrix}(9\times 22)+(2\times 20)\\ (1\times 22)+(15\times 20)\end{bmatrix} = \begin{bmatrix}238\\ 322\end{bmatrix} \ mod\ 26 = \begin{bmatrix}4\\ 10\end{bmatrix}$$

$$\begin{bmatrix}9 & 2\\ 1 & 15\end{bmatrix}\begin{bmatrix}22\\ 25\end{bmatrix} = \begin{bmatrix}(9\times 22)+(2\times 25)\\ (1\times 22)+(15\times 25)\end{bmatrix} = \begin{bmatrix}248\\ 397\end{bmatrix} \ mod\ 26 = \begin{bmatrix}14\\ 7\end{bmatrix}$$

$$\begin{bmatrix}9 & 2\\ 1 & 15\end{bmatrix}\begin{bmatrix}6\\ 25\end{bmatrix} = \begin{bmatrix}(9\times 6)+(2\times 25)\\ (1\times 6)+(15\times 25)\end{bmatrix} = \begin{bmatrix}104\\ 381\end{bmatrix} \ mod\ 26 = \begin{bmatrix}0\\ 17\end{bmatrix}$$

$$\begin{bmatrix}9 & 2\\ 1 & 15\end{bmatrix}\begin{bmatrix}16\\ 23\end{bmatrix} = \begin{bmatrix}(9\times 16)+(2\times 23)\\ (1\times 16)+(15\times 23)\end{bmatrix} = \begin{bmatrix}190\\ 361\end{bmatrix} \ mod\ 26 = \begin{bmatrix}8\\ 23\end{bmatrix}$$

Setelah didapatkan matriks *plaintext*, konversikan matriks tersebut sesuai dengan tabel indeks alfabet.

$$\begin{bmatrix}E\\ K\end{bmatrix} = \begin{bmatrix}4\\ 10\end{bmatrix}$$
$$\begin{bmatrix}O\\ H\end{bmatrix} = \begin{bmatrix}14\\ 7\end{bmatrix}$$
$$\begin{bmatrix}A\\ R\end{bmatrix} = \begin{bmatrix}0\\ 17\end{bmatrix}$$
$$\begin{bmatrix}I\\ X\end{bmatrix} = \begin{bmatrix}8\\ 23\end{bmatrix}$$

TUGAS

- SOAL :

1. Plaintext :

SUKA UDINUS

- Silahkan di enkripsi dan di Dekripsi
- Matriks Kunci : $\begin{bmatrix} 7 & 14 \\ 20 & 11 \end{bmatrix}$

2. Plaintext :

10 Nama digit nama anda

- Silahkan di enkripsi dan di Dekripsi

Matriks Kunci : $\begin{bmatrix} 7 & 14 \\ 20 & 11 \end{bmatrix}$

TERIMAKASIH

Materi Minggu depan: Transposisi