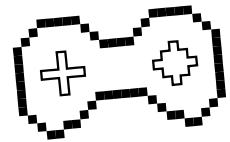
Praktikum Kriptografi

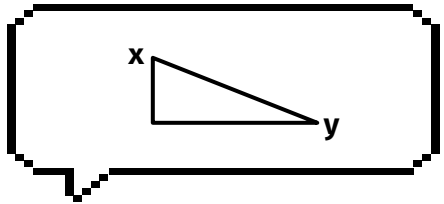
Pertemuan - 03

Topik: Hill Cipher

Review



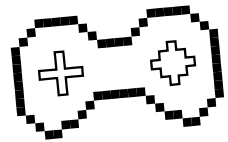
1. **Shift Cipher?**
2. **ROT 13?**
3. **Affine Cipher?**



01

Hill Cipher

Hill Cipher

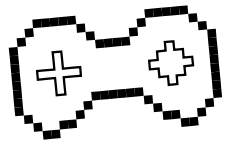


Hill Cipher merupakan salah satu algoritma kriptografi yang memanfaatkan **matriks sebagai kunci** untuk melakukan enkripsi dan dekripsi serta aritmatika modulo.

Syarat Kunci :

- Bisa di-invers-kan (determinan $\neq 0$)
- Jumlah baris dan kolom matriks sama (misal 2×2)
- Jumlah baris dan kolomnya merupakan bilangan prima terkecil yang menjadi faktor dari jumlah karakter yang akan dienkripsi

Enkripsi Hill Cipher



1. Tentukan **Plaintext** (Pt), dan **konversi** ke dalam bentuk angka
2. Susun **plaintext** dalam bentuk **blok matriks** (2×1 jika ordo kunci 2×2, 3×1 jika ordo kunci 3×3)
3. Tentukan **matriks kunci K** (nilai determinan harus ganjil positif / negatif, **selain 13**, karena 13 tidak koprima dengan 26)
4. Lakukan proses enkripsi dengan rumus :

$$C = M_k * M_p$$

Keterangan:

C = *Ciphertext*

M_k = Matriks Kunci

M_p = Matriks *Plaintext*

Contoh Enkripsi Hill Cipher

Diketahui:

Plaintext (Pt) = KRIPTO

$$K = \begin{bmatrix} 3 & 2 \\ 2 & 7 \end{bmatrix}$$

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

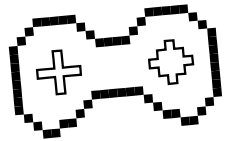
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Solusi:

1. Pt = KRIPTO = **10 17 8 15 19 14**
2. Membagi huruf menjadi beberapa matriks

K	R	I	P	T	O
10	17	8	15	19	14
Matriks 1		Matriks 2		Matriks 3	

Contoh Enkripsi Hill Cipher



Solusi:

3. Determinan matriks kunci $\begin{vmatrix} 3 & 2 \\ 2 & 7 \end{vmatrix}$ = (3*7) - (2*2) = 21 - 4 = 17 (Ganjil)
4. Lakukan perkalian matriks K dan Pt

$$\begin{bmatrix} 3 & 2 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 10 \\ 17 \end{bmatrix} = \begin{bmatrix} 64 \\ 139 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 9 \end{bmatrix} \quad \mathbf{M}\ \mathbf{J}$$

$$\begin{bmatrix} 3 & 2 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 8 \\ 15 \end{bmatrix} = \begin{bmatrix} 54 \\ 121 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 17 \end{bmatrix} \quad \mathbf{C}\ \mathbf{R}$$

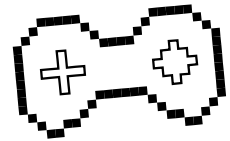
$$\begin{bmatrix} 3 & 2 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 19 \\ 14 \end{bmatrix} = \begin{bmatrix} 85 \\ 136 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 6 \end{bmatrix} \quad \mathbf{H}\ \mathbf{G}$$

Sehingga didapatkan:

KRIPTO ⇒ E(x) ⇒ **MJCRHG**

K	R	I	P	T	O
10	17	8	15	19	14

Exercise



Enkripsikan **PYTHON** dengan K = $\begin{bmatrix} 7 & 6 \\ 2 & 5 \end{bmatrix}$

Tuliskan setiap langkah-langkahnya!

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

Dekripsi Hill Cipher

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

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow \det A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

3. Tentukan nilai **invers modulo**
4. Tentukan **invers** matriks **kunci K**

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

5. Tentukan kunci dekripsi Hill Cipher K^{-1}

Nilai Invers Modulo x *Invers Matriks Kunci*

6. Rumus dekripsi Hill Cipher

$$P = Mk^{-1} * Mc$$

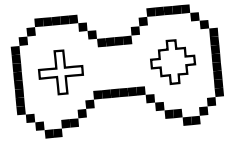
Keterangan:

P = *Plaintext*

M_k^{-1} = Matriks *Kunci Invers*

M_c = Matriks *Ciphertext*

Contoh Dekripsi Hill Cipher



Diketahui:

1. Ciphertext (Ct) = **MJCRHG**
2. K = $\begin{bmatrix} 3 & 2 \\ 2 & 7 \end{bmatrix}$

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

Solusi:

1. Membuat matriks Ct

M	J	C	R	H	G
12	9	2	17	7	6

2. Menentukan determinan matriks K

$$\begin{vmatrix} 3 & 2 \\ 2 & 7 \end{vmatrix} = (3*7) - (2*2) = 21 - 4 = \mathbf{17}$$

3. Menentukan invers modulo

$17^{-1} \bmod 26 \rightarrow \gcd(17, 26) = \mathbf{1}$

Contoh Dekripsi Hill Cipher

Solusi:

GCD(17, 26) = 1
26 = 17 * **1** + 9
17 = 9 * **1** + 8
9 = 8 * **1** + 1
8 = 1 * 8 + 0

4. Tentukan invers matriks kunci K

$$\begin{bmatrix} 3 & 2 \\ 2 & 7 \end{bmatrix}^{-1} = \frac{1}{\det(K)} \begin{bmatrix} 7 & -2 \\ -2 & 3 \end{bmatrix} \bmod 26$$

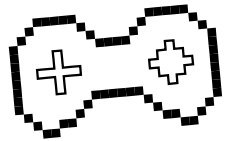
5. Menentukan **matriks K baru** Hill Cipher

$$\begin{bmatrix} 3 & 2 \\ 2 & 7 \end{bmatrix}^{-1} = 23 \cdot \begin{bmatrix} 7 & -2 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 161 & -46 \\ -46 & 69 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 & 6 \\ 6 & 17 \end{bmatrix}$$

Solusi:

t0 = 0
t1 = 1
t2 = t0 – (q1 · t1) mod 26
= 0 – (1 . 1) = –1 mod 26 = 25
t3 = t1 – (q2 · t2) mod 26
= 1 – (1 . 25) = –24 mod 26 = 2
t4 = t2 – (q3 · t3) mod 26
= 25 – (1 . 2) = 23 mod 26 = **23**

Contoh Dekripsi Hill Cipher



Solusi:

4. Melakukan proses dekripsi Hill Cipher

$$\begin{bmatrix} 5 & 6 \\ 6 & 17 \end{bmatrix} \begin{bmatrix} 12 \\ 9 \end{bmatrix} = \begin{bmatrix} 114 \\ 225 \end{bmatrix} \bmod 26 = \begin{bmatrix} 10 \\ 17 \end{bmatrix} \quad \mathbf{K}\ \mathbf{R}$$

$$\begin{bmatrix} 5 & 6 \\ 6 & 17 \end{bmatrix} \begin{bmatrix} 2 \\ 17 \end{bmatrix} = \begin{bmatrix} 112 \\ 301 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 15 \end{bmatrix} \quad \mathbf{I}\ \mathbf{P}$$

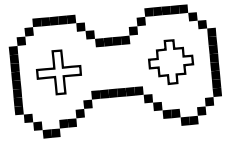
$$\begin{bmatrix} 5 & 6 \\ 6 & 17 \end{bmatrix} \begin{bmatrix} 7 \\ 6 \end{bmatrix} = \begin{bmatrix} 71 \\ 144 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 14 \end{bmatrix} \quad \mathbf{T}\ \mathbf{O}$$

MJCRHG ⇒ D(x) ⇒ **KRIPTO**

M	J	C	R	H	G
12	9	2	17	7	6

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

Mencari Kunci Hill Cipher



Diketahui:

Pt = FRIDAY ; Ct = PQCFKU ; m =2

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

Solusi:

FRIDAY → (5, 17, 8, 3, 0, 24);

PQCFKU → (15, 16, 2, 5, 10, 20)

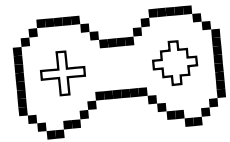
Maka,

$e_k(5,17) = (15,16)$; $e_k(8,3) = (2,5)$; $e_k(0,24) = (10,20)$

K = C . P^{-1}

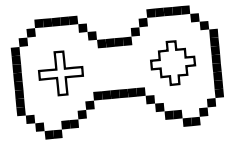
$$K = \begin{bmatrix} 15 & 2 \\ 16 & 5 \end{bmatrix} \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}^{-1} = \begin{bmatrix} 137 & 149 \\ 60 & 107 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$$

Tugas



1. Kumpulkan Exercise (dalam format pdf) tadi di Classroom
2. Buatlah program untuk enkripsi, dekripsi, dan mencari kunci Hill Cipher (bahasa pemrograman bebas)
3. Push program tersebut ke repository **NPM-Kripto23** dan sertakan juga screenshot di dalamnya.
4. Jelaskan program yang sudah dibuat di dalam 1 file pdf lalu kumpulkan di classroom

Instruksi Tugas



Tugas Penjelasan Program:

Format: Tugas3_NPM.pdf

Exercise :

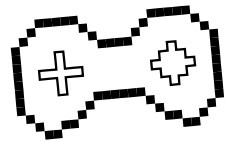
Format: Exercise3_NPM.pdf

Tugas Program :

Format Repo GitHub: NPM-Kripto23

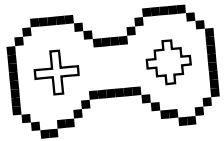
Format Folder: Hill-Cipher, **Format File:** hillcipher.<ext>

Deadline Tugas: H-1 Praktikum Berikutnya, 23.59



Reminder!!

Minggu depan ada kuis, silakan persiapkan materinya dari **pertemuan 1** sampai **pertemuan 3**



Thank You!!

Kalau misalkan ada pertanyaan,
yaudah tanya aja

Praktikum Kriptografi 2022