
Kriptografi
MATRIKS IN TECH

Encrypt

Kriptografi Hill Cipher

Definisi Kriptografi

Melakukan perubahan kata asli untuk melindungi pesan tersebut

Hill Cipher :

Mengubah sebuah kata menjadi bentuk kalimat acak dengan mengkodekan hurufnya ke dalam angka

Penerapan Matriks

Operasi Matriks, Indeks Matriks dan Invers Matriks

Komponen

Key, Plain Text, Cipher Text

Bidang Penerapan

Militer

Kriptografi Hill Cipher

Definisi Kriptografi

Melakukan perubahan kata asli untuk melindungi pesan tersebut

Hill Cipher :

Mengubah sebuah kata menjadi bentuk kalimat acak dengan mengkodekan hurufnya ke dalam angka

Penerapan Matriks

Operasi Matriks, Indeks Matriks dan Invers Matriks

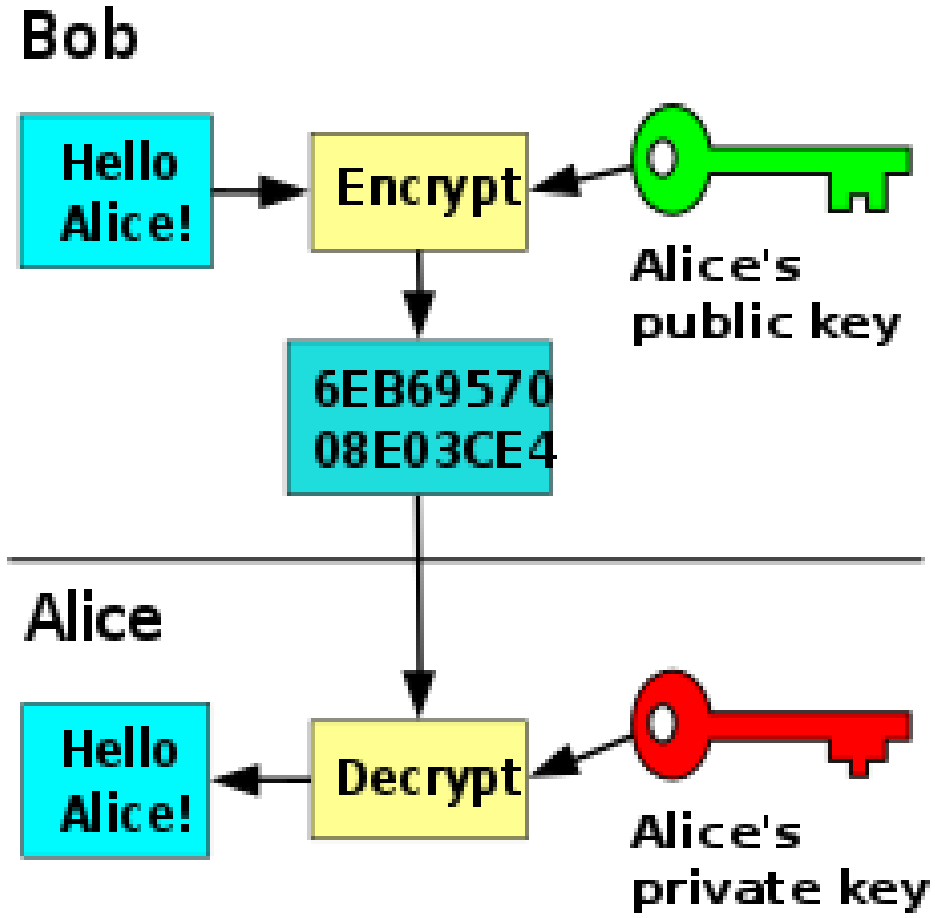
Komponen

Key, Plain Text, Cipher Text

Bidang Penerapan

Militer

Prinsip Kriptografi



Istilah Dalam Kriptografi

- **Plaintext** (P) adalah pesan yang hendak dikirimkan (berisi data asli).
- **Ciphertext** (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
- **Enkripsi** (fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
- **Dekripsi** (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
- **Kunci** adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Pengkodean

_	.	A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13

M	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	26	27

Konversi Plain Text

P : SISTEM

P : 20 10 20 21 6 14

_	.	A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13

M	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	26	27

Buat Matriks Kunci

$$K = \begin{bmatrix} 1 & 5 \\ 9 & 8 \end{bmatrix}$$

Blok Plain Text

P : SISTEM

P : 20 10 20 21 6 14

- $P = \begin{bmatrix}20\\10\end{bmatrix}\begin{bmatrix}20\\21\end{bmatrix}\begin{bmatrix}6\\14\end{bmatrix}$

- $P_{1,2} = \begin{bmatrix}20\\10\end{bmatrix}$
- $P_{3,4} = \begin{bmatrix}20\\21\end{bmatrix}$
- $P_{5,6} = \begin{bmatrix}6\\14\end{bmatrix}$

Kalikan dengan Matriks Kunci

- $C_{1,2} = K \,.\, P_{1,2}(mod\ (jumlah\ karakter\ yang\ dikodekan))$

- $C_{1,2} = \begin{bmatrix} 1 & 5 \\ 9 & 8 \end{bmatrix} . \begin{bmatrix} 20 \\ 10 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 70 \\ 260 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 14 \\ 8 \end{bmatrix}$
- $C_{3,4} = \begin{bmatrix} 1 & 5 \\ 9 & 8 \end{bmatrix} . \begin{bmatrix} 20 \\ 21 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 125 \\ 348 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 13 \\ 12 \end{bmatrix}$
- $C_{5,6} = \begin{bmatrix} 1 & 5 \\ 9 & 8 \end{bmatrix} . \begin{bmatrix} 6 \\ 14 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 76 \\ 166 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 20 \\ 26 \end{bmatrix}$

Buat Urutan

- $C1, C2, C3, C4, C5, C6$
- C = 14 8 13 12 20 26
- C = MGLKSY

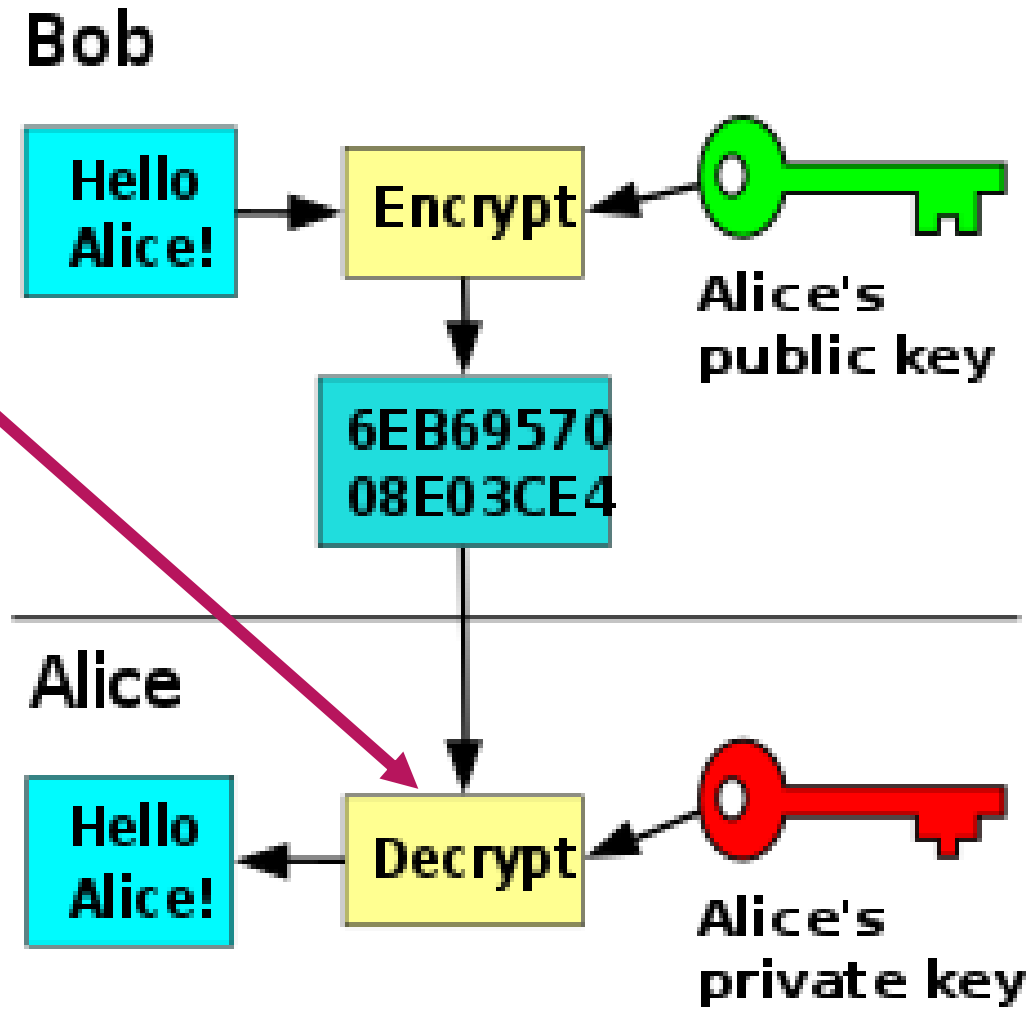
_	.	A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13

M	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	26	27

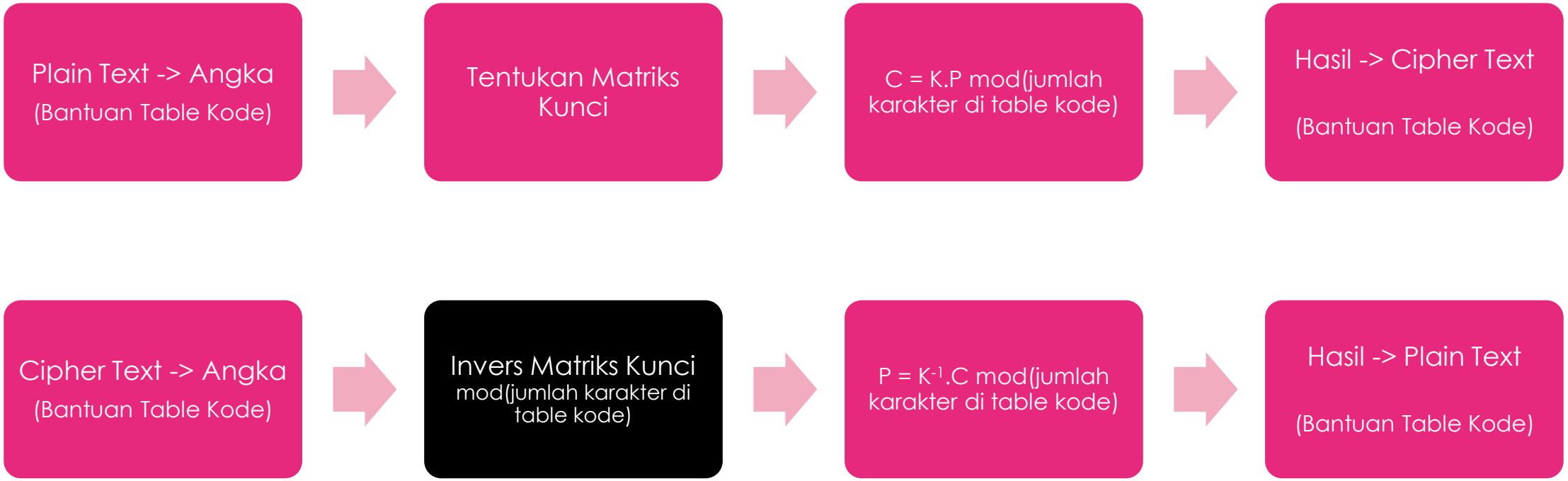
- $C_{1,2} = \begin{bmatrix} 14 \\ 8 \end{bmatrix}$
- $C_{3,4} = \begin{bmatrix} 13 \\ 12 \end{bmatrix}$
- $C_{5,6} = \begin{bmatrix} 20 \\ 26 \end{bmatrix}$

Decrypt

Posisi kita


Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

Apa bedanya dengan Encrypt



Invers Matriks

Invers matriks adalah **sebuah kebalikan (invers)** dari kedua matriks di mana apabila matriks tersebut dikalikan menghasilkan matriks identitas (AB = BA = I)

Pembuktian

A.B = B.A = 1 (Matriks Identitas)

$$A = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} \quad B = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$$

$$AB = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \text{ (matriks identitas)}$$

$$BA = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \text{ (matriks identitas)}$$

Maka dapat dituliskan bahwa $B = A^{-1}$ (B Merupakan *invers* dari A

OBE

- Operasi Baris Elementer
  - Perkalian elemen baris dengan scalar (scalar tidak boleh 0)
  - Operasi penjumlahan dan pengurangan antar elemen pada baris yang berbeda

Contoh Soal

A.B = B.A = 1 (Matriks Identitas)

A.B = 1
Jika B tidak diketahui
sama saja dengan

B = 1/A
B = 1 * A^{-1}

Matriks A $\begin{matrix} 2 & 1 \\ 3 & 2 \end{matrix}$ → $\begin{matrix} 2 & 1 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{matrix}$

1. B1/2

$$\begin{bmatrix} 1 & ½ & ½ & 0 \\ 3 & 2 & 0 & 1 \end{bmatrix}$$

2. B2-(B1*3)

$$\begin{bmatrix} 1 & ½ & ½ & 0 \\ 0 & ½ & -3/2 & 1 \end{bmatrix}$$

3. B2*2

$$\begin{bmatrix} 1 & ½ & ½ & 0 \\ 0 & 1 & -3 & 2 \end{bmatrix}$$

4. B1-(B2/2)

$$\begin{bmatrix} 1 & 0 & \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix} \\ 0 & 1 & \end{bmatrix}$$

→ B Invers A

https://penma2b.wordpress.com/2016/07/03/invers-matriks-3x3-obe-gancu-kunci/

Cipher Text

- C = MGLKSQ

_	.	A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13

M	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	26	27

Sama dengan table kode yang ditentukan saat akan melakukan enkripsi

Konversi Cipher Text

C = MGLKSY

C = 14 8 13 12 20 26

_	.	A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13

M	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	26	27

Invers Matriks Kunci

- Matriks Kunci yang sama dengan proses Encrypt

$$[K|I] = \left[\begin{array}{cc|cc} 1 & 5 & 1 & 0 \\ 9 & 8 & 0 & 1 \end{array}\right]$$

Proses Invers Matriks Kunci

$$[K|I] = \left[\begin{array}{cc|cc} 1 & 5 & 1 & 0 \\ 9 & 8 & 0 & 1 \end{array}\right] (3 \times R2) = \left[\begin{array}{cc|cc} 1 & 5 & 1 & 0 \\ 27 & 24 & 0 & 3 \end{array}\right]$$

$$= \left[\begin{array}{cc|cc} 1 & 5 & 1 & 0 \\ -1 & 24 & 0 & 3 \end{array}\right] (R2 + R1) = \left[\begin{array}{cc|cc} 1 & 5 & 1 & 0 \\ 0 & 29 & 1 & 3 \end{array}\right]$$

$$= \left[\begin{array}{cc|cc} 1 & 5 & 1 & 0 \\ 0 & 1 & 1 & 3 \end{array}\right] (R1 + (-5 \times R2)) = \left[\begin{array}{cc|cc} 1 & 0 & -4 & -15 \\ 0 & 1 & 1 & 3 \end{array}\right]$$

Invers Matriks Kunci Modulus

$$= \left[\begin{array}{cc|cc} 1 & 0 & -4 & -15 \\ 0 & 1 & 1 & 3 \end{array}\right] \ (mod\ 28)$$

$$= \left[\begin{array}{cc|cc} 1 & 0 & 24 & 13 \\ 0 & 1 & 1 & 3 \end{array}\right]$$

Dari perhitungan di atas, maka didapat $K^{-1} = \begin{bmatrix} 24 & 13 \\ 1 & 3 \end{bmatrix}$

Blok Cipher Text

C : MGLKSQ

C : 14 8 13 12 20 18

- $C = \begin{bmatrix}14\\8\end{bmatrix}\begin{bmatrix}13\\12\end{bmatrix}\begin{bmatrix}20\\26\end{bmatrix}$

- $C_{1,2} = \begin{bmatrix}14\\8\end{bmatrix}$
- $C_{3,4} = \begin{bmatrix}13\\12\end{bmatrix}$
- $C_{5,6} = \begin{bmatrix}20\\26\end{bmatrix}$

Kalikan dengan Invers Matriks Kunci

- $P_{1,2} = K^{-1} . C_{i,j}(mod\ (jumlah\ karakter\ yang\ dikodekan))$

- $P_{1,2} = \begin{bmatrix} 24 & 13 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 14 \\ 8 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 440 \\ 38 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 20 \\ 10 \end{bmatrix}$
- $P_{3,4} = \begin{bmatrix} 24 & 13 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 13 \\ 12 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 468 \\ 49 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 20 \\ 21 \end{bmatrix}$
- $P_{5,6} = \begin{bmatrix} 24 & 13 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 20 \\ 26 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 818 \\ 98 \end{bmatrix} (\text{mod } 28) = \begin{bmatrix} 6 \\ 14 \end{bmatrix}$

Buat Urutan

- P1, $P2, P3, P4, P5, P6$
- C = 20 10 20 21 6 14
- C = S I S T E M

_	.	A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13

M	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	26	27

- $P_{1,2} = \begin{bmatrix} 20 \\ 10 \end{bmatrix}$
- $P_{3,4} = \begin{bmatrix} 20 \\ 21 \end{bmatrix}$
- $P_{5,6} = \begin{bmatrix} 6 \\ 14 \end{bmatrix}$

$$K = \begin{bmatrix} 1 & 5 \\ 9 & 8 \end{bmatrix}$$

_	.	A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13

M	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	26	27

C = MGLKSY

C = 14 8 13 12 20 26

P : SISTEM

P : 20 10 20 21 6 14

Terima Kasih