No ~~2~~ 1 Satu

Matriks K 2x2

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

Cek det: $\det(k) = (3 \times 5 - 3 \times 2) = 15 - 6 = 9 \neq 0$

$GCD(9, 26) = 1$ $\cancel{\neq 0}$

Plaintext = BAJANGRIAUAS

Proses Enkripsi

$$C = K \cdot P \mod 26$$

blok 1: $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \times 3 + 3 \times 0 \\ 2 \times 1 + 5 \times 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$

Blok 2: $\begin{bmatrix} 3 \times 9 + 3 \times 0 \\ 2 \times 9 + 5 \times 0 \end{bmatrix} = \begin{bmatrix} 27 \\ 18 \end{bmatrix} \mod 26 = \begin{bmatrix} 1 \\ 18 \end{bmatrix}$

Blok 3: $\begin{bmatrix} 3 \times 13 + 3 \times 6 \\ 2 \times 13 + 5 \times 6 \end{bmatrix} = \begin{bmatrix} 57 \\ 56 \end{bmatrix} \mod 26 = \begin{bmatrix} 5 \\ 4 \end{bmatrix}$

Blok 4: $\begin{bmatrix} 3 \times 17 + 3 \times 8 \\ 2 \times 17 + 5 \times 8 \end{bmatrix} = \begin{bmatrix} 75 \\ \cancel{80}\ 74 \end{bmatrix} \mod 26 = \begin{bmatrix} 23 \\ \cancel{8}\ 22 \end{bmatrix}$

Blok 5: $\begin{bmatrix} 3 \times 0 + 3 \times 20 \\ 2 \times 0 + 5 \times 20 \end{bmatrix} = \begin{bmatrix} 60 \\ 100 \end{bmatrix} \mod 26 = \begin{bmatrix} 8 \\ 22 \end{bmatrix}$

Blok 6: $\begin{bmatrix} 3 \times 0 + 3 \times 18 \\ 2 \times 0 + 5 \times 18 \end{bmatrix} = \begin{bmatrix} 54 \\ 90 \end{bmatrix} \mod 26 = \begin{bmatrix} 2 \\ 12 \end{bmatrix}$

Diperoleh Chipertext =

[3, 2] → D C

[1, 18] → B S

[5, 10] → F ~~K~~ E

[23, 8] → X I

[8, 22] → I W

[2, 12] → C M

Proses deskripsi

$k = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$ dengan $det(k) = 9$

$9 \times d \equiv 1 \pmod{26}$

$9 \times 3 = 27 \equiv 1 \pmod{26}$

$det(k)^{-1} \equiv 3 \pmod{26}$

Matriks adj

$$adj(k) = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

konversi elemen negatif mod 26:

$-3 \equiv 26 - 3 = 23 \pmod{26}$

$-2 \equiv 26 - 2 = 24 \pmod{26}$

$$adj(k) = \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} \pmod{26}$$

Matriks invers k^{-1}

$$k^{-1} = det(k)^{-1} \times adj(k) \pmod{26}$$

$$k^{-1} = 3 \times \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} = \begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix} \bmod 26$$

Hitung mod 26 tiap elemen

- $15 \bmod 26 = 15$
- $69 \bmod 26 = 69 - 2 \times 26 = 69 - 52 = 17$
- $72 \bmod 26 = 72 - 2 \times 26 = 72 - 52 = 20$
- $9 \bmod 26 = 9$

Jadi $k^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$

$$\text{blok 1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 3 \\ 2 \end{bmatrix}$$

$$= \begin{bmatrix} 15 \times 3 + 17 \times 2 \\ 20 \times 3 + 9 \times 2 \end{bmatrix} = \begin{bmatrix} 45 + 34 \\ 60 + 18 \end{bmatrix} = \begin{bmatrix} 79 \\ 78 \end{bmatrix} \text{mod } 26$$

hitung modulonya =

- $79 \text{ mod } 26 = 79 - 3 \times 26 = 79 - 78 = 1$
- $78 \text{ mod } 26 = 78 - 3 \times 26 = 78 - 78 = 0$

jadi blok 1 = [1, 0]
[B, A]

$$\text{blok 2} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 1 \\ 18 \end{bmatrix}$$

$$= \begin{bmatrix} 15 \times 1 + 17 \times 18 \\ 20 \times 1 + 9 \times 18 \end{bmatrix} = \begin{bmatrix} 15 + 306 \\ 20 + 162 \end{bmatrix} = \begin{bmatrix} 321 \\ 182 \end{bmatrix}$$

Hitung modulo 26 =

- $321 \text{ mod } 26 = 321 - 12 \times 26 = 321 - 312 = 9$
- $182 \text{ mod } 26 = 182 - 7 \times 26 = 182 - 182 = 0$

blok 2 = [9, 0]
(J, A)

$$\text{Blok 3} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 5 \\ \cancel{23}\ 4 \end{bmatrix} = \begin{bmatrix} 75 + \cancel{391}\ 68 \\ \cancel{100 + 207}\ 100 + 36 \end{bmatrix} = \begin{bmatrix} \cancel{466}\ 143 \\ \cancel{307}\ 136 \end{bmatrix}$$

mod 26

- $\cancel{466 \text{ mod } 26} = \cancel{466} - 7 \times 26 = 466 - \cancel{442 = 24}$
- $\cancel{307 \text{ mod } 26 = 307 - 11 \times 26 = 307 - 286} = 21$

blok 3 = [~~24~~, 21]

mod 26 = [17, 8]
[R, I]

blok 4 (23, 22)

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 23 \\ 22 \end{bmatrix} = \begin{bmatrix} 345 + 374 \\ 460 + 198 \end{bmatrix} = \begin{bmatrix} 719 \\ 658 \end{bmatrix} = \begin{bmatrix} 17 \\ 8 \end{bmatrix}$$

R, I

blok 5 (8, 22)

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 8 \\ 22 \end{bmatrix} = \begin{bmatrix} 120 + 374 \\ 160 + 198 \end{bmatrix} = \begin{bmatrix} 494 \\ 358 \end{bmatrix} = \begin{bmatrix} 0 \\ 20 \end{bmatrix}$$

A U

blok 6 (2, 12)

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 2 \\ 12 \end{bmatrix} = \begin{bmatrix} 30 + 204 \\ 40 + 108 \end{bmatrix} = \begin{bmatrix} 234 \\ 148 \end{bmatrix} = \begin{bmatrix} 0 \\ 18 \end{bmatrix}$$

Hasil = [0, 18] [A, S]

No.

Date

matriks 3x3.

$$k = \begin{bmatrix} 2 & 5 & 7 \\ 11 & 13 & 17 \\ 19 & 23 & 29 \end{bmatrix}$$

P : KOMPUTERLIINEAR.

Tabel 2.1 (A = 0, B = 1, ..., Z = 25).

M = 12, K = 10, A = 0, L = 11, J = 9
A = 0, B = 1, A = 0, R = 17, L = 11, I
= 8, N = 13, E = 4, A = A = 0, R = 17.

Blok 1 = 12 10 0.
Blok 2 = 11 9 0
Blok 3 = 1 0 17.
Blok 4 = 11 8 13
Blok 5 = 4 0 17.

rumus Hill Cipher C = K * P mod 26

Blok 1.

No

Date

$C_1 = (2 \cdot 12 + 5 \cdot 10 + 7 \cdot 0) \bmod 26 =$
$(24 + 50 + 0) \bmod 26 = 74 \bmod 26$
$= 22$
$C_2 = (11 \cdot 12 + 13 \cdot 10 + 17 \cdot 0) \bmod 26 = (132 +$
$130 + 0) \bmod 26 = 262 \bmod 26 = 12$

Blok 2.

$C_4 = (2 \cdot 11 + 5 \cdot 9 + 7 \cdot 0) \bmod 26 = (22 + 4$
$+ 0) \bmod 26 = 67 \bmod 26 = 15$
$C_5 = (11 \cdot 11 + 13 \cdot 9 + 17 \cdot 0) \bmod 26 = (121 + 117$
$0) \bmod 26 = 238 \bmod 26 = 4$
$C_6 = (19 \cdot 11 + 23 \cdot 9 + 23 \cdot 0) \bmod 26 =$
$(209 + 207 + 0) \bmod 26 = 416$
$\bmod 26 = 0$

Blok 3.

$C_7 = (2 \cdot 1 + 5 \cdot 0 + 7 \cdot 17) \bmod 26 = (2 + 0 + 119$
$\bmod 26 = 121 \bmod 26 = 17$
$C_8 = (11 \cdot 1 + 13 \cdot 0 + 17 \cdot 17) \bmod 26 =$
$(11.70 + 289) \bmod 26 = 512 \bmod 26 \doteq$

No.

Date

Blok 4

$C_{10} = (2 \cdot 11 + 5 \cdot 8 + 7 \cdot 13) \bmod 26 =$
$(22 + 40 + 91) \bmod 26 = 153$
$\bmod 26 = 23.$

$C_{11} = (11 \cdot 11 + 13 \cdot 8 + 17 \cdot 13) \bmod 26$
$= (121 + 104 + 221) \bmod 26 =$
$\bmod 26 = 6.$

$C_{12} = (19 \cdot 11 + 23 \cdot 8 + 29 \cdot 13) \bmod 26$
$= (209 + 184 + 377) \bmod 26 = 770$
$\bmod 26 = 8.$

Blok 5 :

$C_{13} = 2 \cdot 4 + 5 \cdot 0 + 7 \cdot 17) \bmod 26$
$(8 + 0 + 199 \bmod 26 = 127 \bmod 26$
$= 23$

$C_{14} = (11 \cdot 4 + 13 \cdot 0 + 17 \cdot 17) \bmod 26$
$= (44 + 0 + 289 \bmod 26 = 333 \bmod$
$26 = 5$

$C_{15} = (19$

No = 3

$$K = \begin{bmatrix} 3 & 3 & 1 & 2 \\ 2 & 5 & 4 & 1 \\ 1 & 6 & 4 & 2 \\ 1 & 7 & 3 & 5 \end{bmatrix}$$

$$\text{blok}_1 = \begin{bmatrix} 1 \\ 0 \\ 9 \\ 0 \end{bmatrix} \quad \text{blok}_2 = \begin{bmatrix} 13 \\ 6 \\ 17 \\ 8 \end{bmatrix} \quad \text{blok}_3 = \begin{bmatrix} 0 \\ 20 \\ 0 \\ 18 \end{bmatrix}$$

Enkripsi

blok 1

$$C_1 = \begin{bmatrix} 3 & 3 & 1 & 2 \\ 2 & 5 & 4 & 1 \\ 1 & 6 & 4 & 2 \\ 1 & 7 & 5 & 5 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 9 \\ 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 3\times1 + 3\times0 + 1\times9 + 2\times0 \\ 2\times1 + 5\times0 + 4\times9 + 1\times0 \\ 1\times1 + 6\times0 + 4\times9 + 2\times0 \\ 1\times1 + 7\times0 + 3\times9 + 5\times0 \end{bmatrix} = \begin{bmatrix} 3+0+9+0 \\ 2+0+36+0 \\ 1+0+36+0 \\ 1+0+27+0 \end{bmatrix} = \begin{bmatrix} 12 \\ 38 \\ 37 \\ 28 \end{bmatrix}$$

mod 26

$$\text{blok } 1 = \begin{bmatrix} 12 \\ 12 \\ 11 \\ 2 \end{bmatrix}$$

---

blok 2 =

$$C_2 = \begin{bmatrix} 3\times13 + 3\times6 + 1\times17 + 2\times8 \\ 2\times13 + 5\times6 + 4\times14 + 1\times8 \\ 1\times13 + 6\times6 + 4\times17 + 2\times8 \\ 1\times13 + 7\times6 + 3\times17 + 5\times8 \end{bmatrix}$$

$$= \begin{bmatrix} 39 + 18 + 17 + 16 \\ 26 + 30 + 68 + 8 \\ 13 + 36 + 68 + 16 \\ 13 + 42 + 51 + 40 \end{bmatrix} = \begin{bmatrix} 90 \\ 132 \\ 133 \\ 146 \end{bmatrix} \overset{\text{mod } 26}{=} \begin{bmatrix} 12 \\ 2 \\ 3 \\ 16 \end{bmatrix}$$

block 3

$$c_3 = \begin{bmatrix} 3\times 0 + 3\times 20 + 1 \times 0 + 2\times 18 \\ 2\times 0 + 5\times 20 + 4 \times 0 + 1\times 18 \\ 1\times 0 + 6\times 20 + 4 \times 0 + 2\times 18 \\ 1\times 0 + 7\times 20 + 3\times 0 + 5\times 18 \end{bmatrix}$$

$$= \begin{bmatrix} 0 + 60 + 0 + 36 \\ 0 + 100 + 0 + 18 \\ 0 + 120 + 0 + 36 \\ 0 + 140 + 0 + 90 \end{bmatrix} = \begin{bmatrix} 96 \\ 118 \\ 156 \\ 230 \end{bmatrix} \bmod 26 = \begin{bmatrix} 18 \\ 14 \\ 0 \\ 22 \end{bmatrix}$$

ciphertext 1, 2, 3 = $\begin{bmatrix} 12 \\ 12 \\ 11 \\ 12 \\ 12 \\ 2 \\ 3 \\ 16 \\ 18 \\ 14 \\ 0 \\ 22 \end{bmatrix} \begin{bmatrix} M \\ M \\ L \\ L \\ M \\ C \\ D \\ Q \\ S \\ O \\ A \\ W \end{bmatrix}$