tugas pertemuan 10
535230080 - Georgià Sugisandhea
→ pesan = DO NOT WALK DOG

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

1. Caesar Cipher dengan $k = 17$

- encrypting

plain text = DO NOT WALK DOG
= 3 14 13 14 19 22 0 11 10 3 14 6

kunci rahasia $k = 17$

$c = (p + k) \bmod 26$
$c = (3 + 17) \bmod 26 = 20$ ⇒ u
$c = (14 + 17) \bmod 26 = 5$ ⇒ f
$c = (13 + 17) \bmod 26 = 4$ ⇒ e
$c = (14 + 17) \bmod 26 = 5$ ⇒ f
$c = (19 + 17) \bmod 26 = 10$ ⇒ k
$c = (22 + 17) \bmod 26 = 13$ ⇒ n
$c = (0 + 17) \bmod 26 = 17$ ⇒ r
$c = (11 + 17) \bmod 26 = 2$ ⇒ c
$c = (10 + 17) \bmod 26 = 1$ ⇒ b
$c = (3 + 17) \bmod 26 = 20$ ⇒ u
$c = (14 + 17) \bmod 26 = 5$ ⇒ f
$c = (6 + 17) \bmod 26 = 23$ ⇒ x

ciphertext = ufefknrcbufx

- decrypting

cipher text = ufefknrcbufx
20 5 4 5 10 13 17 2 1 20 5 23

$p = (c - k) \bmod 26$
$p = (20 - 17) \bmod 26 = 3$ ⇒ d
$p = (5 - 17) \bmod 26 = 14$ ⇒ o
$p = (4 - 17) \bmod 26 = 13$ ⇒ n
$p = (5 - 17) \bmod 26 = 14$ ⇒ o
$p = (10 - 17) \bmod 26 = 19$ ⇒ t
$p = (13 - 17) \bmod 26 = 22$ ⇒ w
$p = (17 - 17) \bmod 26 = 0$ ⇒ a
$p = (2 - 17) \bmod 26 = 11$ ⇒ l
$p = (1 - 17) \bmod 26 = 10$ ⇒ k
$p = (20 - 17) \bmod 26 = 3$ ⇒ d
$p = (5 - 17) \bmod 26 = 14$ ⇒ o
$p = (23 - 17) \bmod 26 = 6$ ⇒ g

plain text = do not walk dog

2. Affine Cipher dengan $a = 17$ dan $b = 5$

- encrypting

plain text = DO NOT WALK DOG
= 3 14 13 14 19 22 0 11 10 3 14 6

kunci rahasia : $a = 17$ dan $b = 5$

$c = (ap + b) \bmod 26$
$c = (17 \cdot 3 + 5) \bmod 26 = 4$ ⇒ e
$c = (17 \cdot 14 + 5) \bmod 26 = 9$ ⇒ j
$c = (17 \cdot 13 + 5) \bmod 26 = 18$ ⇒ s
$c = (17 \cdot 14 + 5) \bmod 26 = 9$ ⇒ j
$c = (17 \cdot 19 + 5) \bmod 26 = 16$ ⇒ q
$c = (17 \cdot 22 + 5) \bmod 26 = 15$ ⇒ p
$c = (17 \cdot 0 + 5) \bmod 26 = 5$ ⇒ f
$c = (17 \cdot 11 + 5) \bmod 26 = 10$ ⇒ k
$c = (17 \cdot 10 + 5) \bmod 26 = 19$ ⇒ t
$c = (17 \cdot 3 + 5) \bmod 26 = 4$ ⇒ e
$c = (17 \cdot 14 + 5) \bmod 26 = 9$ ⇒ j
$c = (17 \cdot 6 + 5) \bmod 26 = 3$ ⇒ d

cipher text : ejsjqpfktejd

- decrypting

cipher text = ejsjqpfktejd
4 9 18 9 16 15 5 10 19 4 9 3

$p = \bar{a}(c - b) \pmod{26}$
$\bar{a}$ = inverse dari 17 modulo 26

$$\left.\begin{aligned} 26 &= 1 \cdot 17 + 9 \\ 17 &= 1 \cdot 9 + 8 \\ 9 &= 1 \cdot 8 + 1 \end{aligned}\right\} \begin{aligned} 9 &= 26 - 1 \cdot 17 \\ 8 &= 17 - 1 \cdot 9 \\ 1 &= 9 - 1 \cdot 8 \end{aligned}$$

↳ $1 = 9 - 1 \cdot (17 - 1 \cdot 9)$
$1 = 2 \cdot 9 - 1 \cdot 17$
$1 = 2 \cdot (26 - 1 \cdot 17) - 1 \cdot 17$
$1 = 2 \cdot 26 \boxed{-3}\, 17$
$\bar{a} = -3$

$p = -3(4 - 5) \bmod 26 = 3$ ⇒ d
$p = -3(9 - 5) \bmod 26 = 14$ ⇒ o
$p = -3(18 - 5) \bmod 26 = 13$ ⇒ n
$p = -3(9 - 5) \bmod 26 = 14$ ⇒ o
$p = -3(16 - 5) \bmod 26 = 19$ ⇒ t
$p = -3(15 - 5) \bmod 26 = 22$ ⇒ w
$p = -3(5 - 5) \bmod 26 = 0$ ⇒ a
$p = -3(10 - 5) \bmod 26 = 11$ ⇒ l
$p = -3(19 - 5) \bmod 26 = 10$ ⇒ k
$p = -3(4 - 5) \bmod 26 = 3$ ⇒ d
$p = -3(9 - 5) \bmod 26 = 14$ ⇒ o
$p = -3(3 - 5) \bmod 26 = 6$ ⇒ g

plain text = do not walk dog ←

3. Transposition Cipher dengan $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, dan $\sigma(4) = 2$

- encrypting

plain text : DO NOT WALK DOG

| D O N O | T W A L | K D O G |

cipher text : O O D N W L T A D G K O

- decrypting

$\sigma^{-1}(1) = 2$ $\sigma^{-1}(3) = 1$

$\sigma^{-1}(2) = 4$ $\sigma^{-1}(4) = 3$

| O O D N | W L T A | D G K O |

plain text : D O N O T W A L K D O G

4. Cryptography

kunci rahasia $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}$ plain text : DO NOT WALK DOG

$A^{-1} = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix}$

→ encrypting

1. "DON" : 3 14 13

$P_1 = \begin{bmatrix} 3 \\ 14 \\ 13 \end{bmatrix}$ $C_1 = A \times P_1 = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 3 \\ 14 \\ 13 \end{bmatrix} = \begin{bmatrix} 70 \\ 66 \\ 99 \end{bmatrix}$ mod 26 $= \begin{bmatrix} 18 \\ 14 \\ 21 \end{bmatrix}$ ⇒ S O V

2. "OTW" = 14 19 22

$P_2 = \begin{bmatrix} 14 \\ 19 \\ 22 \end{bmatrix}$ $C_2 = A \times P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 14 \\ 19 \\ 22 \end{bmatrix} = \begin{bmatrix} 118 \\ 107 \\ 184 \end{bmatrix}$ mod 26 $= \begin{bmatrix} 14 \\ 3 \\ 2 \end{bmatrix}$ ⇒ O D C

3. "ALK" = 0 11 10

$P_3 = \begin{bmatrix} 0 \\ 11 \\ 10 \end{bmatrix}$ $C_3 = A \times P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 11 \\ 10 \end{bmatrix} = \begin{bmatrix} 52 \\ 51 \\ 66 \end{bmatrix}$ mod 26 $= \begin{bmatrix} 0 \\ 25 \\ 14 \end{bmatrix}$ ⇒ A Z O

4. "DOG" = 3 14 6

$P_4 = \begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix}$ $C_4 = A \times P_4 = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix} = \begin{bmatrix} 49 \\ 38 \\ 99 \end{bmatrix}$ mod 26 $= \begin{bmatrix} 23 \\ 12 \\ 21 \end{bmatrix}$ ⇒ X M V

cipher text = SOV ODC AZO XMV

→ decrypting

1. "SOV" = 18 14 21

$C_1 = \begin{bmatrix} 18 \\ 14 \\ 21 \end{bmatrix}$ $P_1 = A^{-1} \times C_1 = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix} \begin{bmatrix} 18 \\ 14 \\ 21 \end{bmatrix} = \begin{bmatrix} -75 \\ 66 \\ -13 \end{bmatrix}$ mod 26 $= \begin{bmatrix} 3 \\ 14 \\ 13 \end{bmatrix}$ ⇒ DON

2. "ODC" = 14 3 2

$C_2 = \begin{bmatrix} 14 \\ 3 \\ 2 \end{bmatrix}$ $P_2 = A^{-1} \times C_2 = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix} \begin{bmatrix} 14 \\ 3 \\ 2 \end{bmatrix} = \begin{bmatrix} -272 \\ 227 \\ -56 \end{bmatrix}$ mod 26 $= \begin{bmatrix} 14 \\ 19 \\ 22 \end{bmatrix}$ ⇒ OTW

3. "AZO" = 0 25 14

$C_3 = \begin{bmatrix} 0 \\ 25 \\ 14 \end{bmatrix}$ $P_3 = A^{-1} \times C_3 = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 25 \\ 14 \end{bmatrix} = \begin{bmatrix} 520 \\ -431 \\ 114 \end{bmatrix}$ mod 26 $= \begin{bmatrix} 0 \\ 11 \\ 10 \end{bmatrix}$ ⇒ ALK

4. " XMV " : 23 12 21

$$C_4 = \begin{bmatrix} 23 \\ 12 \\ 21 \end{bmatrix} \quad P_4 = A^{-1} \times C_4 = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix} \begin{bmatrix} 23 \\ 12 \\ 21 \end{bmatrix} = \begin{bmatrix} -231 \\ 196 \\ -46 \end{bmatrix} \bmod 26 = \begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix} \Rightarrow \text{DOG}$$

plain text = DONOTWALK DOG