

**Tugas 2 Praktikum  
Kriptografi  
Kelas A Semester Ganjil 2021/2022**

**Oleh:**  
WAFI FAHRUZZAMAN – 140810200009



**PROGRAM STUDI S-1 TEKNIK INFORMATIKA  
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM  
UNIVERSITAS PADJADJARAN  
2022**

**Buat satu kalimat sederhana (min 3 kata & total min 15 huruf), enkripsikan dengan Affine Cipher dan kembalikan menjadi plainteks.**

Kalimat : WAFI FAHRUZ ZAMAN

$a = 3$

$b = 12$

$m = 26$

## Enkripsi

Plaintext	W	A	F	I
X	22	0	5	8
$(a \cdot X + b) \bmod 26$	0	12	1	10
Ciphertext	A	M	B	K

F	A	H	R	U	Z
5	0	7	17	20	25
1	12	7	11	20	9
B	M	H	L	U	J

Z	A	M	A	N
25	0	12	0	13
9	12	22	12	25
J	M	W	M	Z

Hasilnya Enkripsi adalah **A M B K B M H L U J J M W M Z**

## Dekripsi

Mencari  $a^{-1}$ :

- GCD(a, m)

GCD(3, 26)

$$26 = 3 \cdot 8 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2 + 0$$

- $t_0 = 0$  ,  $t_1 = 1$

$$t_2 = (t_0 - (q_1 \cdot t_1)) \bmod 26$$

$$\begin{aligned} t_2 &= (0 - (8 \cdot 1)) \bmod 26 \\ &= 18 \end{aligned}$$

$$\begin{aligned} t_3 &= (t_1 - (q_2 \cdot t_2)) \bmod 26 \\ &= (1 - (1 \cdot 18)) \bmod 26 \\ &= 9 \end{aligned}$$

$$a^{-1} = 9$$

<b>Ciphertext</b>	A	M	B	K
<b>Y</b>	0	12	1	10
<b><math>(a^{-1} (Y - b)) \bmod 26</math></b>	22	0	5	8
<b>Plaintext</b>	W	A	F	I

B	M	H	L	U	J
1	12	7	11	20	9
5	0	7	17	20	25
F	A	H	R	U	Z

J	M	W	M	Z
9	12	22	12	25
25	0	12	0	13
Z	A	M	A	N

<b>Hasilnya Dekripsi adalah</b>	<b>W</b>	<b>A</b>	<b>F</b>	<b>I</b>	<b>F</b>	<b>A</b>	<b>H</b>	<b>R</b>	<b>U</b>	<b>Z</b>	<b>Z</b>	<b>A</b>	<b>M</b>	<b>A</b>	<b>N</b>
---------------------------------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------