QUIZ

PRAKTIKUM KRIPTOGRAFI

Disusun Oleh:

Prames Ray Lapian – 140810210059

PROGRAM STUDI S-1 TEKNIK INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PADJADJARAN

JATINANGOR

2021

1. **RSA**

Plain Text : Prames

p : 59

q : 89

Jawab:

RSA							
p	59						
q	89						
Menghitung n dan m							
n	5251						
m	5104						
Memilih e yang relatif prima dengan m							
e	23						
Menghitung d = e^-1 mod m							
GCD							
5104	=	23	*	**221**	+	21	
23	=	21	*	**1**	+	2	
21	=	2	*	**10**	+	1	
2	=	1	*	**2**	+	0	
1	=	0	*	**#DIV/0!**	+	#DIV/0!	
t(0)	=	0					
t(1)	=	1					
t(2)	=	4883					

t(3)	=	222					
t(4)	=	2663	=	e^-1	=	d	
Diperoleh Pasangan Kunci							
publik	(e,n)	=	23	5251			
privat	(d,n)	=	2663	5251			
Enkripsi							
m	P	R	A	M	E	S	
	80	82	65	77	69	83	
	808265776983	12 Digit, sehingga dapat dibagi menjadi 4 berukuran 3 digit					
	808	265	776	983			
	m1	m2	m3	m4			
c	80	1244	2556	805			
	c1	c2	c3	c4			
Dekripsi							
m	80	1244	2556	805			
	m1	m2	m3	m4			
c	808	265	776	983			
p	808265776983						
	80	82	65	77	69	83	
	P	R	A	M	E	S	

2. S-DES

Plain Text : 5 → 00110101

Master Key : 9 → 0011100110

P_{10} : 3 5 2 7 4 10 1 9 8 6

P_8 : 6 3 7 4 8 5 10 9

P_4 : 2 4 3 1

Generate Key dengan P_{10}:

KEY	0	0	1	1	1	0	0	1	1	0
P_{10}	3	5	2	7	4	10	1	9	8	6
Hasil	1	1	0	0	1	0	0	1	1	0

Bagi 2 : 11001 ||| 00110

Ls1 : 10011 ||| 01100

Generate Key dengan P_8:

P_8	6	3	7	4	8	5	10	9
K1	0	0	1	1	1	1	0	0

Ls2 : 01110 ||| 10001

Generate Key dengan P_8:

P_8	6	3	7	4	8	5	10	9
K2	1	1	0	1	0	0	1	0

Enkripsi:00110101

PText	0	0	1	1	0	1	0	1
IP	2	6	3	1	4	8	5	7
Hasil IP	0	1	1	0	1	1	0	0

IP (4-Bit)	1	1	0	0				
EP	4	1	2	3	2	3	4	1
Hasil EP	0	1	1	0	1	0	0	1

EP	0	1	1	0	1	0	0	1
K1	0	0	1	1	1	1	0	0
Hasil XOR	0	1	0	1	0	1	0	1

S_0 : 0101 R_n : 01 C_n : 10

S_1 : 0101 R_n : 01 C_n : 10

3.

$$y^2 \equiv x^3 + 7x + 10 \ (mod\ 23)$$

$$y1 = qa$$

$$= 2\ (16,\ 3)$$

$$= (16,\ 3) + (16,\ 3)$$

$$\lambda = \frac{3x_1 + q}{2y_1}$$

$$= \frac{3\ .\ 256 + 1}{2\ .\ 3}$$

$$= 769, 4\ mod\ 23$$

$$= 17$$

$$x^3 = \lambda^2 - x_1 - x_2$$

$$= 17^2 - 16 - 16$$

$$= 257\ mod\ 23$$

$$= 4$$

$$y^2 = \lambda\ (x_1 - x_3) - y_1$$

$$= 17(16 - 4) - 3$$

$$= 201\ mod\ 23$$

$= 17$

$y_1 = (4, 17)$

$y_2 = (p_!, p_2) + q(r.\alpha)$

$= (4, 7) + 2(3.\alpha)$

$3\alpha = 2\alpha + \alpha$

$= (4, 17) + (16, 3)$

$\lambda = \frac{3-17}{16-4} = \frac{-14}{12} \, mod \, 23$

$= -14 . 2 \, mod \, 23$

$= 18$

4.

5.

6. Tugas