Nama : Jeans Prima Simaremare
NIM : 14117018
UAS Kriptografi.

1. Dik $p = 101$, $q = 103$ } untuk nilai $n = p * q$
$= 101 * 103$
$= 10.403$

Plain text → I AM SORRY. → 73, 32, 65, 77, 32, 83, 79, 82, 82, 89.

Dit. a. pilih kunci enkripsi yang memenuhi

Hitung nilai $\phi(n) = (p-1)(q-1)$
$= (101-1)(103-1)$
$= (100)(102)$
$= 10.200$

Untuk nilai e $= (e, 10.200) = 1$

Kita pilih $e = 19$. Sedemikian sehingga relatif prima terhadap $\phi(n) = 10.200$ kurang dari $\phi(n)$ Nilai $d = 6979$.

b. I = 73

$C = m^e \bmod n$ (fungsi enkripsi)

$C = 73^{19} \bmod 10403 = 8679$

Spasi → $C = 32^{19} \bmod 10403 = 6625$

A (65) → $C = 65^{19} \bmod 10403 = 5367$

M (77) → $C = 77^{19} \bmod 10403 = 5301$

Spasi (32) → $C = 32^{19} \bmod 10403 = 6625$

S (83) → $C = 83^{19} \bmod 10403 = 9422$

O (79) → $C = 79^{19} \bmod 10403 = 6653$

R (82) → $C = 82^{19} \bmod 10403 = 10.398$

R (82) → $C = 82^{19} \bmod 10403 = 10.398$

Y (89) → $C = 89^{19} \bmod 10403 = 7323$

Maka kita Mendapatkan nilai C = 6625 5367 5301 6625 9422 6653 10.398 10398 7323

C. Kunci dekripsi yang bersesuaian

R (82) = 10.398 ⇒ C.

$M = C^d \bmod n$. (fungsi Dekripsi)

$M = 10.398^{6979} \bmod 10.403$

M = 82.

2. Dik N = 199

g = 18 → Nim 2 angka dari belakang

x = 32

Y = 24 → Tanggal lahir

$X = g^x \bmod n = 18^{32} \bmod 199 = 188$

$Y = g^Y \bmod n = 18^{24} \bmod 199 = 125$

$k = Y^x \bmod n = 125^{32} \bmod 199 = 121$

$k = X^Y \bmod n = 188^{24} \bmod 199 = 121$

Maka kunci simetri yang digunakan adalah $k = 121$

3. $y^2 = x^3 + 16x + 10 \pmod{17}$ B = Bulan lahir +1 → Bulan 9

Titik Basis.

Kunci Privat = [9, 16]

b = 9 + 1 = 10

Pb = bB

k = 5

Pesan akhir (15,15), Pm = (15,15)

a. Pc = [(kB), (Pm + kPB)]

= E.

b. Pm = (Pm + kPB) − (b(kB)) = Pm + k(bB − bkB)

4. Plaintext state

49	20	61	6d
20	73	6f	72
72	79	70	66
6f	72	30	35

⊕

round key

49	20	68	6f
70	65	20	79
6f	75	20	68
61	70	70	79

=

State

0	0	9	2
50	16	4f	1b
1d	c	0	e
e	2	40	4c