Question 4

Menggunakan $p = 5$ dan q 11, lakukan ekripsi RSA dgn Inisial nama dan kemudian lakukan dekripsi

jawab : $p = 5$

$q = 11$

inisial nama = MPS

* Enkripsi

$m = p \cdot q = 5 \cdot 11 = 55$

$\varnothing(55) = \varnothing(5 \cdot 11) = 4 \cdot 10 = 40$

$e = 3$

kunci publik = $(3, 55)$

* MPS ⇒ $M = 13$, $P = 16$, $S = 19$

$C = B^e \bmod m$

$C = B^3 \bmod 55$

Jadi

Plain	B	B^3	Cipertext
M	13	2197	52
P	16	4096	26
S	19	6859	39

blok Cipertext = 52 26 39

180 mm x 257 mm

KIK

D. dekripsi

* membuat kunci privat

$m = p \cdot q = 55$

$5 \cdot 11$

$\phi m = \phi(55) = \phi(5 \cdot 11) = 4 \cdot 10 = 40$

$d \cdot e = 1 \mod \phi m$

$d \cdot 3 = 1 \mod 40$

$3d \equiv 1 \mod 40$

$d = \gcd(3,40)$

$40 = 3 \cdot 13 + 1$

$3 = 1 \cdot 3 + 0$

$1 = 40 - 3 \cdot 13$

$B = c^d \mod m$

C	C^{13}	$B = c^d \mod m$	plain
52	20325604e+22	13	M
26	24811529e+18	16	P
39	48288075e+20	19	S