Date.....

Qu: 1 a)

we need to find out,

$4^{283} \bmod 10$

⇒

$4^1 \,\%\, 10 = 4$
$4^2 \,\%\, 10 = 6$
$4^3 \,\%\, 10 = 4$
$4^4 \,\%\, 10 = 6$

Note % = mod

⇒ $4^n \,\%\, 10$ will have 2 value based on n

i.e

$$4^n \,\%\, 10 = \begin{cases} 4 & n = \text{odd} \\ 6 & n = \text{even} \end{cases}$$

So, $4^{283} \,\%\, 10 = 4$ Ans

Qu: 1 b) find $9^{682} \bmod 10$

following same strategy as Q 1.a)

$9^1 \,\%\, 10 = 9$
$9^2 \,\%\, 10 = 1$
$9^3 \,\%\, 10 = 9$
⋮

again % = mod

$$9^n \,\%\, 10 = \begin{cases} 9 & n\,\%\,2 = 1 \ (\text{odd}) \\ 1 & n\,\%\,1 = 0 \ (\text{even}) \end{cases}$$

$9^{682} \,\%\, 10 = 1$

Ans

Date.....

Qu: 2 $p = 61$ and $q = 71$ (2)

Sol Step 1 $n = p \times q$

$= 61 \times 71$

Step 2

and $\phi(n) = (p-1) \times (q-1)$

$\Rightarrow 60 \times 70$

$= 4200$

Step 3 we need to find an 'e' such that

$1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$

So, e is the smallest encryption exponent that can be chosen by A

$\gcd(11, 4200) = 1$

or $e = 11$

Step 4 decryption component

$d = e^{-1} \bmod \phi(n)$

or $d = 2291$

i.e

$2291 \times 11 = 25201$

and

$25201 \% 4200 = 1$ (one)

Date.....

Q 3 Given that

$p = 79, \quad g = 3$

A private key = 5 = x

B private key = 27 = y

formula for common secret = $g^{xy} \bmod p$

$\Rightarrow 3^{35} \bmod 79$

find

$3^3 = 27$

$3^5 \% 79 = 6$

$3^7 \% 79 = 54$

$3^{14} \% 79 = 72$

$3^{28} \% 79 = 49$

$3^{35} \% 79 = 39$

OR

$3^{35} \bmod 79 = 39$