RSA

i) 2 prime no p, q

ii) $n = p \times q$

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

iv) a) $1 < e < \phi(n)$

b) e, $\phi(n)$ are coprime

v) Calculate d

$(d * e) \bmod n = 1$

Public key = {e, n}

Private key = {d, n}

Encryption

$C = M^e \bmod n$

Decryption

$M = C^d \bmod n$

Q) M = Hello

e = 3, n = 33

Ans

i) p & q ✓

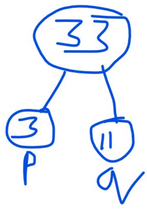
$n = p \times q$

$33 = p \times q$

$33 = 3 \times 11$

$\therefore p = 3$

$q = 11$



---

ii) n = 33 ✓

iii) $\phi(n) = (p-1)(q-1)$ ✓

$= (3-1)(11-1)$

$= 2 \times 10$

$\phi(n) = 20$

---

iv) a) $1 < e < \phi(n)$ ✓

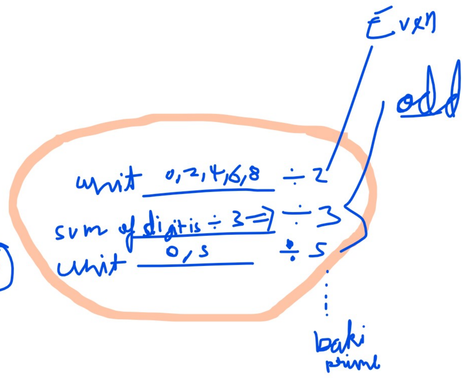
$1 < 3 < 20$ ✓

b) e, $\phi(n)$ are coprime

3, 20

$3 = 1 \times 3$

$20 = 1 \times 2 \times 2 \times 5$



20