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

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

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 ✓

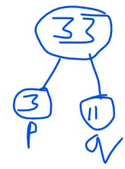
$n = p \times q$

$33 = p \times q$

$33 = 3 \times 11$

$\therefore p = 3$

$q = 11$



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) are coprime ✓

v) Calculate d

$(d \times e) \bmod \phi(n) = 1$

$(d \times 3) \bmod 20 = 1$

calculator $(e * x - 1) \div \phi(n) = ?$

$(3 * x - 1) \div 20 = 7$

$d = 7$

1 → 3 − 1 = 2 and − 20 — ✗

2 → 3 − 20, E − 40 — ✗

3

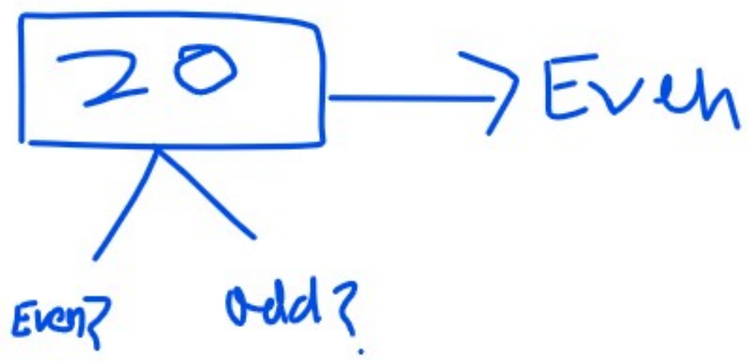
Prime Numbers 1 to 100

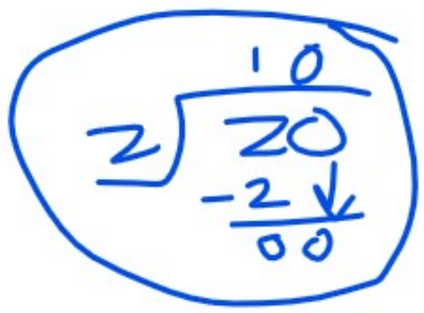
2 3 5 7 11 13 17 19

23 29 31 37 41 43 47

53 59 61 67 71 73 79

83 89 97





baki prime

Unitdigit → 0, 2, 4, 6, 8

2 ÷