p = 7

q = 13

n = 7 \* 13 = 91

phi(n) = 6 \* 12 = 71

**e = 1**

GCD(72,1) = q 72 r 0

Not secure

**e = 2**

GCD(72,2) = q 26 r 0

72 and 2 are not co-prime

**e = 3**

GCD(72,3) = q 24 r 0

72 and 3 are not co-prime

**e = 4**

GCD(72,4) = q 18 r 0

72 and 4 are not co-prime

**e = 5**

GCD(72,5) = q 14 r 2 => 2 = 72(1) + 5(-14)

GCD(5,2) = q 2 r 1 => 1 = 5(1) + 2(-2)

= 5(1) + 72(-2) + 5(28)

= 5(29) + 72(-2)

=> d = 29

**e = 6**

GCD(72,6) = q 12 r 0

72 and 6 are not co-prime

**Only e =5 and d= 29 is good**

**Public key = {e, n} = {5, 91}**

**Private key = {d, n} = {29, 91}**