Euler's Totient Function, denoted as ϕ(n)

ϕ(n) = Num of positive integers less than n, that are relatively prime to n

ϕ(7) = ?

We will check co-prime relationship of 7 with 1,2,3,4,5,6

GCD(1,7) = 1 ==>1 & 7 co-prime

GCD(2,7) = 1 ==>2 & 7 co-prime

GCD(3,7) = 1 ==>3 & 7 co-prime

GCD(4,7) = 1 ==>4 & 7 co-prime

GCD(5,7) = 1 ==>5 & 7 co-prime

GCD(6,7) = 1 ==>6 & 7 co-prime

So, ϕ(7) = 6.

ut ϕ(367) = ?

We will check co-prime relation of 1,2,3,4, ... 365,366 with 367 ????

No.....................

Formula:

For ϕ(n):

1.If n is prime, then ϕ(n) = n-1

2.If n can be divided as

n = p x q, and p & q are primes,

then ϕ(n) = n-1

3. If n can e divided as n = a x b, where a or b or both are composite num, then

$\phi(n) = n \times (1 - 1/P1) \times (1 – 1/P2) \ldots$, here P1, P2, … are distinct primes

2. Fermat's Little Theorem

Fermat's Little Theorem states that if p is a prime and a is an integer not divisible by p, then:

$a^{(p-1)} \equiv 1 \pmod{p}$

Example:

For a = 2 and p = 7:

2^(7-1) = 2^6 = 64

64 mod 7 = 1

Thus, 2^6 ≡ 1 (mod 7) 3.

3. Euler's Theorem

It states that if a and n are coprime, then:

$a^{\phi(n)} \equiv 1 \pmod{n}$

Example:

For a = 2 and n = 10,

ϕ(10) = 4: 2^4 = 16

16 mod 10 = 1

Thus, 2^4 ≡ 1 (mod 10)

4. RSA Key Generation for p = 311 and q = 317 1.

1. Calculate n:

   n = p × q = 311 × 317 = 9858

2. Compute Euler's Totient Function ϕ(n):
   $\phi(n) = (p - 1) \times (q - 1) = (311 - 1) \times (317 - 1) = (310) \times (316) = 97960$
3. Choose Public Key Exponent e: We need to choose e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.
   first 10 elements of Z_{97960}^{*} are: 1, 3, 9, 11, 17, 19, 23, 29, 31, 33.
   Let's select the 10th elemnt of Z_{97960}^{*}. So choose e = 33
4. Find the Private Key Exponent d: Compute d using the Extended Euclidean Algorithm, which satisfies: $d \times e \equiv 1 \mod \phi(n)$

Q	A	B	R	t1	t2	t
2968	97960	33	16	0	1	-2968
2	33	16	1	1	-2968	5937
16	16	1	0	-2968	5937	-97960
	1	0		5937	97960	

Public key: (e,n)=(33,98587)

Private key: ((d,n)=(5937,98587)

Step 1: Encryption

The encryption formula is:

$C = m^e \mod n$

Where:

- m=10 (the message)
- e=33 (public exponent)
- n=98587

$C = 10^{33} \mod 98587$

C =18490 (How ?? Think ..)

Step 2: Decryption

The decryption formula is:

$M = (c^d) \bmod n$

Where:

- c is the ciphertext (calculated in step 1)
- d=5937 (private exponent)
- n=98587

$m = 18490^{5937} \bmod 98587$