**Internet Security Roleplay**

**Explaining GCD using Euclidean Algorithm**

|  |  |  |
| --- | --- | --- |
| **A** | **B** | **R** |
| 33 | 12 | 9 |
| 12 | 9 | 3 |
| 9 | 3 | 0 |
| 3 | 0 |  |

The **biggest number** should be place in **column A** and **smallest number** should be place in **column B**

* Initially, place 33 in column A and 12 in column B.
* Divide 33 by 12, resulting in a remainder of 9, which is placed in column R.
* After division, shift the numbers to the left: the value in column B shifts to column A, and the value in column R shifts to column B.
* Repeat the division process with the values in columns A and B, placing the remainder in column R.
* Continue this process until column B reaches 0.
* Once column B becomes 0, The value in column A will represent the GCD of 12 and 33.
* If the number is **prime** then the gcd will be always **1** “**GCD(11,3)=1”.**

**Euler Totient Function**

**There are three types of Method:**

|  |  |  |
| --- | --- | --- |
| **Ф(n)** | **Criteria of ‘n’** | **Formula** |
| **‘n’ is prime** | **Ф(n) = (n-1)** |
| **n=p x q**  **‘p’ and ‘q’ are primes** | **Ф(n)=(p-1) x (q-1)** |
| **n = a x b**  **Either ‘a’ or ‘b’ is composite.**  **Both ‘a’ and ‘b’ are composite.** | **Ф(n)=n x (1-1/p1)\*(1-1/p2)…**  **where p1,p2… are distant primes** |

Euler Totient Function is denoted as **Ф(n)**

**Definition:** It is number of positive integers less than ‘n’ that are relatively prime to n

There are three types of Criteria of ‘n’

1) First Criteria says if **‘n’ is prime** the formula will be **Ф(n) = (n-1)**

**Example:**

n=5

n is a prime number

**Ф(n)=(n-1)**

**Ф(5)=(5-1)**

**Ф(5)=4**

2) Second Criteria says If the **“n is the product of two prime numbers”** like **“p” and “q”** so theformula will be **Ф(n)=(p-1) x (q-1)**

**Example:**

n=5

n is a product of two prime numbers **5 and 7**

Let us assign **p=5 and q=7**

**Ф(n)=(p-1)(q-1)**

**Ф(35)=(5-1)(7-1)**

**Ф(35)=4 x 6**

**Ф(35)=24**

**There are 24 numbers that are lesser than 35 and relatively prime to 35**

3) Third Criteria says If the **“n =a x b”** means **“Either a or b is composite or Both a and b are composite”** the formula will be **Ф(n)=n x (1-1/p1)\*(1-1/p2)… where p1,p2… are distant primes**

**Example:**

n=1000

factorization of **1000** = **23 x 53**

**Ф(n)=n x (1-1/p1) (1-1/p2)…**

**Ф(1000)=1000 x (1-1/2) (1-1/5)**

**Ф(1000)=1000 x (1/2) (4/5)**

**Ф(1000)= 400**

**Euler’s Theorem**

For every positive integer ‘a’ & ‘n’, which are said to be relatively prime, then **a^Фn =1 mod n**

**Euler’s theorem a=3 and n=10**

**a^Фn =1 (mod n)**

**3^Ф10 = 1 (mod 10)**

**Ф10 = 4 ….By Applying the Euler Totient Function**

**3^4 = 1 (mod 10)**

**81 = 1 (mod 10)**

Euler Theorem holds true for a=3 and n=10

It provides the mathematical foundation for the RSA algorithm to ensure the security and effectiveness of the encryption scheme. By applying Euler's theorem, RSA ensures that certain mathematical relationships hold true, allowing for secure encryption and decryption of messages using public and private keys.