# SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

**An Autonomous Institution**

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

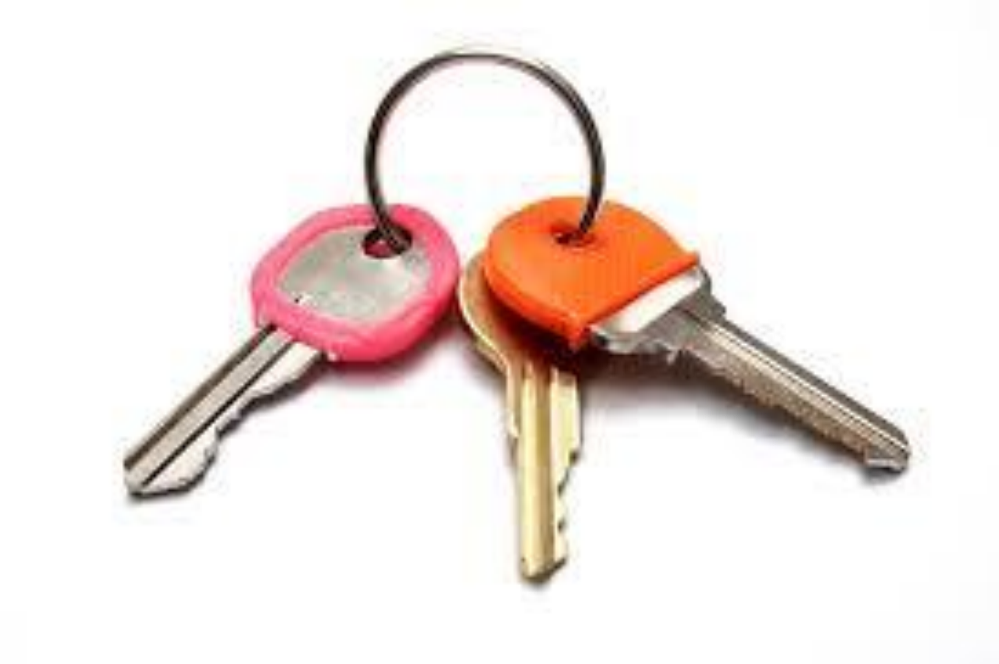
**Course Code and Name : 19CS503 – CRYPTOGRAPHY AND NETWORK SECURITY**

**Unit 3: Public Key Cryptography**

**Topic : Euler's totient function, Fermat's and Euler's Theorem**

# THEOREMS

**FERMAT'S THEOREM** → **EULER'S TOTIENT FUNCTION** → **EULER'S THEOREM**

# FERMAT'S THEOREM

- Useful in public key and primality testing
- If P is Prime Number & a is a positive integer not divisible by p then

$$a^{p-1} = 1 \pmod p$$

- where p is prime and gcd(a,p)=1
- Also known as Fermat's Little Theorem
- Also have: $a^p = a \pmod p$
- **Example**
- $13^{16} \bmod 17 = 1$
- $13^{18} \bmod 17 = 13^{16}\, 13^{2} \bmod 17 = 13^{2} \bmod 17 = 169 \bmod 17=16$

# FERMAT’S THEOREM

$$a = 7, p = 19$$
$$7^2 = 49 \equiv 11 \pmod{19}$$
$$7^4 \equiv 121 \equiv 7 \pmod{19}$$
$$7^8 \equiv 49 \equiv 11 \pmod{19}$$
$$7^{16} \equiv 121 \equiv 7 \pmod{19}$$
$$a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}$$

# EULER'S TOTIENT FUNCTION ø(n)

- Case 1: if n= pq, Where p and q are two prime numbers; p≠q

**ø(n) = pq =ø(p)*ø(q) = (p-1) *(q-1)**

- Case 2: if n is a prime number

**ø(n) = (n-1)**

- Case 3: If n= $p^e$

**ø(n) = $p^e - p^{e-1}$**

- **Example**

□ ø(21) = (3–1)x(7–1) = 2x6 = 12

□ ø(3) = (3-1) = 2

□ ø(8) = $2^3 = 2^3 - 2^2$ = 8-4 = 4

# EULER'S TOTIENT FUNCTION ø(n)

- $\phi(n)$ : How many numbers there are between 1 and $n$-1 that are relatively prime to $n$.
- $\phi(4) = 2$ (1, 3 are relatively prime to 4).
- $\phi(5) = 4$ (1, 2, 3, 4 are relatively prime to 5).
- $\phi(6) = 2$ (1, 5 are relatively prime to 6).
- $\phi(7) = 6$ (1, 2, 3, 4, 5, 6 are relatively prime to 7).

# EULER'S THEOREM

- Every a and n that are relatively prime:

**$a^{ø(n)} \equiv 1 (\text{mod } n)$**

- **Example**
- a=3;n=10; ø(10)=4;

  hence 34 = 81 = 1 mod 10

- a=2;n=11; ø(11)=10;

  hence 210 = 1024 = 1 mod 11

# EULER'S THEOREM

$22^1 = 22$

$22^2 = 484$

$22^3 = 10648$

$22^4 = 234256$

⋮

What is the last digit of

$22^{88}$ ?

# Testing for Primality

- often need to find large prime numbers
- traditionally sieve using trial division

  ie. divide by all numbers (primes) in turn less than the square root of the number

  only works for small numbers
- alternatively can use statistical optimality tests based on properties of primes
- for which all primes numbers satisfy property
- but some composite numbers, called pseudo-primes, also satisfy the property
- can use a slower deterministic Primality test

# Miller Rabin Algorithm

a test based on prime properties that result from Fermat's Theorem algorithm is:

TEST (n) is:

1. Find integers k, q, k > 0, q odd, so that (n–1)=2kq
2. Select a random integer a, 1<a<n–1
3. if aq mod n = 1 then return ("inconclusive");
4. for j = 0 to k – 1 do
5. if (a2jq mod n = n-1)

   then return("inconclusive")
6. return ("composite")

# REFERENCES

William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.

# THANK YOU