INFORMATION SECURITY

Assignment – 2

1) Explain the following theorems.

a. Fermat's Little Theorem

Fermat's little theorem states that if p is a prime number, then for any integer a, the number $a^p – a$ is an integer multiple of p.

$a^p \equiv a \pmod p$

Special Case:

If a is not divisible by p, Fermat's little theorem is equivalent to the statement that $a^{p-1}-1$ is an integer multiple of p.

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

OR

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

Here a is not divisible by p.

Example:

P = an integer Prime number

a = an integer which is not multiple of P

Let a = 2 and P = 17

According to Fermat's little theorem

$2^{17-1} \equiv 1 \bmod(17)$

we got 65536 % 17 ≡ 1

that mean (65536-1) is an multiple of 17

b. Euler's Theorem

According to Euclid Euler Theorem, a perfect number which is even, can be represented in the form (2^n - 1)*(2^n / 2))) where n is a prime number and 2^n – 1 is a Mersenne prime number. It is a product of a power of 2 with a Mersenne prime number. This theorem establishes a connection between a Mersenne prime and an even perfect number.

c. Chinese Remainder Theorem

We are given two arrays num[0..k-1] and rem[0..k-1]. In num[0..k-1], every pair is coprime. We need to find minimum positive number x such that:

x % num[0] = rem[0],

x % num[1] = rem[1],

....

x % num[k-1] = rem[k-1]

Basically, we are given k numbers which are pairwise coprime, and given remainders of these numbers when an unknown number x is divided by them. We need to find the minimum possible value of x that produces given remainders.

Example:

Input: num[] = {5, 7}, rem[] = {1, 3}

Output: 31

Explanation:

31 is the smallest number such that:

(1) When we divide it by 5, we get remainder 1.

(2) When we divide it by 7, we get remainder 3.

Input: num[] = {3, 4, 5}, rem[] = {2, 3, 1}

Output: 11

Explanation:

11 is the smallest number such that:

(1) When we divide it by 3, we get remainder 2.

(2) When we divide it by 4, we get remainder 3.

(3) When we divide it by 5, we get remainder 1.

d. Euler's Totient Function

Euler's Totient function Φ (n) for an input n is the count of numbers in {1, 2, 3, …, n-1} that are relatively prime to n, i.e., the numbers whose GCD (Greatest Common Divisor) with n is 1.

Example:

Φ(1) = 1
gcd(1, 1) is 1
Φ(2) = 1
gcd(1, 2) is 1, but gcd(2, 2) is 2.
Φ(3) = 2
gcd(1, 3) is 1 and gcd(2, 3) is 1
Φ(4) = 2
gcd(1, 4) is 1 and gcd(3, 4) is 1
Φ(5) = 4
gcd(1, 5) is 1, gcd(2, 5) is 1,
gcd(3, 5) is 1 and gcd(4, 5) is 1
Φ(6) = 2
gcd(1, 6) is 1 and gcd(5, 6) is 1