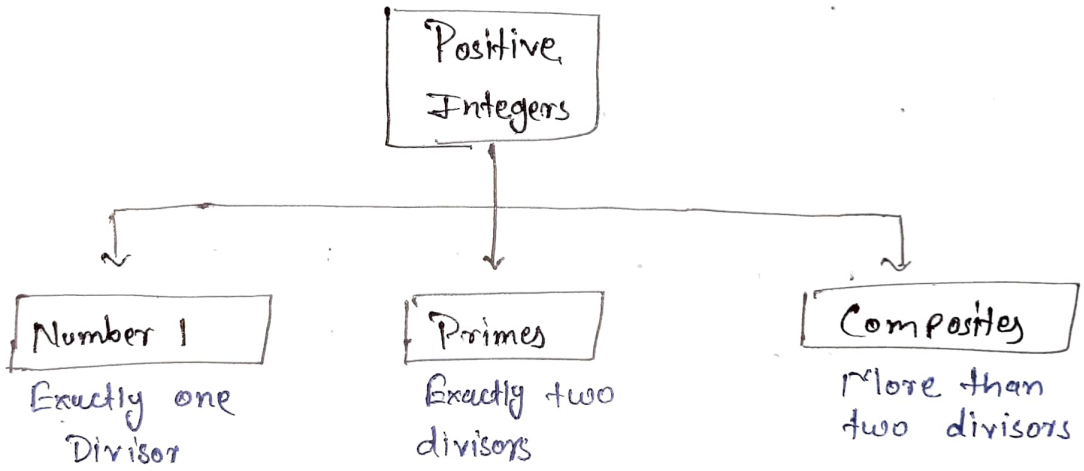
Chapter - 9

Mathematics of cryptography

Primes :- Asymmetric - key cryptography uses Primes extensively.

A Positive integers can be devided into 3 groups

1. number 1,
2. Primes,
3. composites.



Coprimes or relatively prime :- Two Numbers ~~are~~ a, b are coprime if the gcd (a, b) = 1

The Number 1 is relatively prime to with any integer.

If p is prime the all the number 1 — p-1 are coprime to p

Z_n^* :- all member of this set is relatively Prime to n.

Checking for Primeness :- If the number 'n' is Not divisible by all primes less $\sqrt{n}$ the 'n' is a Prime.

Sieve of Eratosthenes :- This is a method to find all primes less than n.

first we write down all the number from 2 to n. & then devide all the numbers by prime numbers less then $\sqrt{n}$.

Example :- $n = 10$ $\sqrt{n} = 3...$

Primes = 2, 3

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

2, 3, 5, 7 are Not divisible by 2 or 3 (execpt 2, 3)
(2, 3 is already prime)

Euler's Phi function :- Euler's Phi function $\phi(n)$, which sometimes called the "Euler's totient function" plays a very important role in cryptography.

This function find the all the numbers relatively Prime to n & Smaller then n.
In other word we have to find Z_n^*.

The function is :-

(1) $\phi(1) = 0$

(2) $\phi(p) = p-1$ { if p is prime }

(3) $\phi(m \times n) = \phi(m) \times \phi(n)$ { where m & n are relatively prime }

(4) $\phi(p^e) = p^e - p^{e-1}$ { If p is prime }

NOTE :- The difficulty of finding $\phi(n)$ depends on the difficulty of finding the factorization of n.

Example :- $\phi(13) = 12$ (Rule 1)

$\phi(10) = \phi(5) \times \phi(2) = 4 \times 1 = 4$ (Rule 3)

$\phi(240) = \phi(2^4) \times \phi(3) \times \phi(5)$

$= [2^4 - 2^3] \times 2 \times 4$

$= 8 \times 8 = 64$ (Rule 4)

$\phi(49) = \phi(7) \times \phi(7) = 36$ (wrong way)

$\phi(49) = 7^2 - 7 = 42$ (Right way)

what is the numbers of element in Z_{14}^*

$\phi(14) = \phi(7) \times \phi(2) = 6.$

Fermat's Little theorem :- This theorem plays an important role in cryptography.

We Have 2 versions of this theorem.

First version :-

If p is Prime & a in any integer & p is Not Divisible by a

then $\boxed{(a^{p-1}) \bmod p \equiv 1 \bmod p}$

Second version :- $\boxed{a^p \bmod p = a \bmod p}$ It removes the condition on 'a'.

It is Helpful in finding some Exponenciation.

Example :- ① $6^{10} \bmod 11 = 1$ (version 1)

② $3^{12} \bmod 11 = (3^{11} \bmod 11 \times 3 \bmod 11) \bmod 11$

$= (3 \times 3) \bmod 11$

$= 9 \bmod 11$

Multiplicative Inverse :- This theorem is useful in finding the multiplicative inverse very quickly.

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

where p is prime, a is integer & $(p \nmid a)$ p does not devide a.

Prove

$$= (a \times a^{-1}) \bmod p$$

$$\Rightarrow [a \bmod p \times a^{-1} \bmod p] \bmod p$$

$$= [a \bmod p \times a^{p-2} \bmod p] \bmod p$$

$$= (a \times a^{p-2}) \bmod p$$

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

$$= 1 \quad \text{(By version 1 of fermate little theorem)}$$

Example:-

$$8^{-1} \bmod 17 = 8^{15} \bmod 17 = 15 \bmod 17$$

Euler's Theorem:- It is a generalized form of fermat's little theorem.

The modulus in the fermat little theorem is a prime. But the modulus in Eular's theorem is an integer.

Similarly we have 2 versions of this theorem.

first version:- This version is similar to first version of fermat little theorem.

$$\left(a^{\phi(n)} \bmod n\right) = 1 \bmod n$$

where a & n are integer

But a & n must be coprime.

Second version:- It is similar to second version of fermat's little theorem.

It removes the condition that a & n should be coprime

$$a^{k \times \phi(n)+1} \bmod n = a \bmod n$$

where k is any integer.

Proof :-

$$a^{k \times \phi(n)+1} \bmod n$$

$$= \left(a^{\phi(n)} \bmod n\right)^k \times a \bmod n$$

$$= 1^k \times a \bmod n$$

$$= a \bmod n.$$

Example

Example :-

find the result of $6^{24} \bmod 35$

$= 6^{\phi(35)} \bmod 35$

$= 1$

find the result of $20^{62} \bmod 77$

$\phi(77) = \phi(7) \times \phi(11)$

$= 6 \times 10$

$= 60$

$= 20^{62} \bmod 77$

$= 20^{\phi(77)+2} \bmod 77$

$= 20^{\phi(77)} \bmod 77 \times 400 \bmod 77$

$= 1 \times 400 \bmod 77$

$= 15$

Multiplicative inverse :- It is useful in finding the multiplicative inverses.

If n & a are coprime then

$$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$$

Example

$8^{-1} \bmod 77 = 8^{60-1} \bmod 77$

$= 8^{59} \bmod 77$

$= 29 \bmod 77$

$= 29$

Generating Primes :- Two Mathematicians, Mersenne and fermat, attempted to develop a formula that could generate Primes.

Mersenne Primes :-

Mersenne defined the following formula

$$M_p = 2^p - 1$$

If p is prime the M_p was thought to be Prime.

NOTE :- But all the number Created using this formula is Not Prime.

~~Example~~

Example :-

$2^2 - 1 = 3$ → (Prime)

$2^3 - 1 = 7$

$2^5 - 1 = 31$

$2^7 - 1 = 127$

$2^{11} - 1 = 2047$ (Not Prime) (23×89)

Fermat Primes :-

Fermat tried to find a formula to generate Primes. The following is the formula for a fermat number

$$F_n = 2^{2^n} + 1$$

{ It gives may or may not Primes }

He tested up to f_4 & got f_5 not prime

Primality testing :- The above schemes are failed to generate large prime number.

But we can choose large number & check whether the number is prime or not.

we have 2 types of algorithm for Primality testing :-

1. Deterministic :- Gives always correct answer
2. Probablistic :- This gives correct answer most of the time But Not all the time.

But Deterministic is less efficient compared to Probablistic one's.

Deterministic Algorithms:-

(1) Divisibility Algorithm :- Divide the given number 'n' with all the Primes less then $\sqrt{n}$ if any of these number is able to divide 'n' then n is composite number.

The number of operation is $O(\sqrt{n})$

If we are performing operation on bits the, the complexity is $O(2^{n_b/2})$

where n_b = Number of bits in n.

This is Exponential time complexity.

(2) AKS algorithm :- This algorithm says that He is able to find whether the no. is Prime or Not in polynomial bit operation which is $O(\log_2 n_b)^{12}$

$(x-a)^p \equiv (x^p - a) \bmod p$ (This algo. uses this fact)

Probablistic Algorithm :- This algorithm give the Prime in polynomial time complexity But it is gaurantee that it allways gives the Right answer.

Rule 1 :- If the number is tested is actually a prime. the algorithm definitely returns a prime.

Rule 2 :- If the number is composite. Then it returns a composite with probablity $1-\varepsilon$ But it may return Prime with Probablity ε

(1) Fermat test :-

The first Probabilistic method we discuss is the Fermat Primality test

> If n is prime then,
> $a^{n-1} \bmod n \equiv 1 \bmod n$

If n is Prime then the relationship hold

It does not mean that, If the congruence hold n is prime.

The integer can be a prime or composite

> If n is prime $a^{n-1} \bmod n \equiv 1 \bmod n$
>
> If n is composite, it is possible $a^{n-1} \bmod n \equiv 1 \bmod n$

A composite may pass the fermat test with Probablity ε.

Example :- Does the number 561 pass the fermat test ?

$$2^{561-1} \equiv 1 \bmod 561$$

This Number passes the fermat test but it is not a prime because $561 = 33 \times 17$.

(2) Square root test :-

Before seeing this test, first we have to understood the concept of square root in modulo operation.

If $x^2 = y \bmod n$

then the squareroot of y is x in mod n.

Example :- Find the square root of 4 is Mod 5.

We know $Z_5 = \{0, 1, 2, 3, 4\}$

$1^2 \bmod 5 = 1$
$2^2 \bmod 5 = 4$
$3^2 \bmod 5 = 4$
$4^2 \bmod 5 = 1$

By above formula 2 & 3 are the Squre root of 4.

We use this concept for checking Prime :-

Given the number 'n'. If it is a Prime. then only $1^2 \bmod n = 1$ & $(n-1)^2 \bmod n = 1$

If we are getting 1 at other place then the given number is not Prime.

Example :-

This means that in case of Prime the square root of 1 is 1 & (n-1)

But in case of composite we got a square root of 1 other then 1 & (n-1)

Example :-

n = 5, 7

$1^2 \bmod 5 = 1$
$2^2 \bmod 5 = 4$
$3^2 \bmod 5 = 4$
$4^2 \bmod 5 = 1$

1 & n-1

~~$5^2 \bmod 5 =$~~

Square root of 1 is 1 & 3
So it is Prime

$1^2 \bmod 7 = 1$
$2^2 \bmod 7 = 4$
$3^2 \bmod 7 = 2$
$4^2 \bmod 7 = 2$
$5^2 \bmod 7 = 4$
$6^2 \bmod 7 = 1$

Square root of 1 is 1 & 6
So 7 is Prime

Example :- $n = 8$

$1^2 \bmod 8 = 1$
$2^2 \bmod 8 = 4$
$3^2 \bmod 8 = 1$
$4^2 \bmod 8 = 0$
$5^2 \bmod 8 = 1$
$6^2 \bmod 8 = 4$
$7^2 \bmod 8 = 1$

the squre root of 1 is 1, 3, 5, 7 other then 1 & n-1 so 8 is Not prime.

Note :- It is Not gaurantee that this test work every time.

Example:

$n = 6$

$1^2 \bmod 6 = 1$
$2^2 \bmod 6 = 4$
$3^2 \bmod 6 = 3$
$4^2 \bmod 6 = 4$
$5^2 \bmod 6 = 1$

Square root of 1 is 1 & n-1 so according to our test 6 is Prime But it is Not.

(3) Miller - Rabin test :- This test combines the format test and the Square root test in a very elegant way.

Algorithm :-

Step 1 :- Find $n-1 = 2^k \times m$

Step 2 :- Choose 'a' such that $1 < a < n-1$

Step 3 :- compute $b_0 = b^m \bmod n$.

if $b_0 = 1$ then n is composite

else if $b_0 = -1$ then n is probably prime we have to stop Here

But if b_0 is ± 1 the we have to compute

$$b_i = b_{i-1}^2 \bmod m$$

then again we check above conditions.

Example :- is 561 is prime ?

$n = 561$

Step 1 :- $n-1 = 2^k \times m$

$560 = 2^4 \times 35$

$k = 4 \quad , m = 35$

Step 2 :- $a = 2$

Step 3 :- $b_0 = 2^{35} \bmod 561 = 263$

$b_1 = (263)^2 \bmod 561 = 166$

$b_2 = (166)^2 \bmod 561 = 67$

$b_3 = (67)^2 \bmod 567 = 1$

means 567 is Not prime it is composite.

Chinese Remainder Theorem :-

The Chinese Remainder theorem is used to Solve a set of congruent equations with one variable but different moduli which are relative Prime.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{m_k}$$

$$X = \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} \cdots a_k M_k M_k^{-1}\right) \pmod{M}$$

$M = a_1 \times a_2 \cdots a_k$

$M_1 = \frac{M}{m_1}$

$M_2 = \frac{M}{m_2}$

$\vdots$

$M_k = \frac{M}{m_k}$

M_i^{-1} = Multiplicative invers of M_i finded using Extended Equlidean algorithm.

Note:- Solution is possible only when $m_1, m_2 \cdots m_k$ are coprime.

Example :-

$x \equiv 2 \bmod 3$
$x \equiv 3 \bmod 5$
$x \equiv 2 \bmod 7$

$a_1 = 2, \quad a_2 = 3, \quad a_3 = 2$
$m_1 = 3, \quad m_2 = 5, \quad m_3 = 7$

$M = 3 \times 5 \times 7 = 105$

$m_1 = \frac{105}{3} = 35 \qquad m_1^{-1} = 2$

$m_2 = \frac{105}{5} = 21 \qquad m_2^{-1} = 1$

$m_3 = \frac{105}{7} = 15 \qquad m_3^{-1} = 1$

$x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$= 233 \bmod 105$

$\boxed{x = 23}$

Modular Exponentiation :-

Example 1 :- Solve ~~$88^7 \mod 187$~~

$$88^7 \mod 187$$

$88^1 \mod 187 = 88$

$88^2 \mod 187 = 88^1 \times 88^1 \mod 187 = 7744 \mod 187$

$= 77$

$88^4 \mod 187 = (88^2 \times 88^2) \mod 187 = (77 \times 77) \mod 187$

$= 5929 \mod 187 = 132$

$88^7 \mod 187 = (88^4 \times 88^2 \times 88^1) \mod 187$

$= (132 \times 77 \times 88) \mod 187$

$= (894432) \mod 187$

$= 11$

Example 2 :-

What is the last two digits of 29^5 = ?

or

Find $29^5 \bmod 100$

$29^1 \bmod 100 = 29$

$29^2 \bmod 100 = (29^1 \times 29^1) \bmod 100 = 41$

$29^4 \bmod 100 = (29^2 \times 29^2) \bmod 100 = (41 \times 41) \bmod 100$

$= 1681 \bmod 100$

$= 81$

$29^5 \bmod 100 = (29^4 \times 29^1) \bmod 100 = (81 \times 29) \bmod 100$

$= 49.$

Example 3 :-

Solve $3^{100} \bmod 29$

$3^1 \bmod 29 = 3$

$3^2 \bmod 29 = 9$

$3^3 \bmod 29 = 27 \bmod 29 = 27$

3^4 mo.

Examples :-

Solve $3^{100} \bmod 29$

$3^1 \bmod 29 = 3$

$3^2 \bmod 29 = (3^1 \times 3^1) \bmod 29 = 9$

$3^4 \bmod 29 = (3^2 \times 3^2) \bmod 29$

$= (9 \times 9) \bmod 29$

$= 81 \bmod 29$

$= 23$ or -6

$3^8 \bmod 29 = (3^4 \times 3^4) \bmod 29$

$= (-6 \times -6) \bmod 29$

$= 36 \bmod 29$

$= 7$

$3^{16} \bmod 29 = (3^8 \times 3^8) \bmod 29$

$= (7 \times 7) \bmod 29$

$= 49 \bmod 29$

$= 20$ or -9

$3^{32} \bmod 29 = (3^{16} \times 3^{16}) \bmod 29$

$= (-9 \times -9) \bmod 29$

$= 81 \bmod 29$

$= 23$ or -6

$3^{64} \bmod 29 = (3^{32} \times 3^{32}) \bmod 29$

$= (-6 \times -6) \bmod 29$

$= 36 \bmod 29$

$= 7 \bmod 29$

$= 7$

$3^{100} = (3^{64} \times 3^{32} \times 3^{4}) \bmod 29$

$= (7 \times -6 \times -6) \bmod 29$

$= (7 \times 36) \bmod 29$

$= (7 \times 7) \bmod 29$

$= 49 \bmod 29$

$= 20.$

Example :- $23^{16} \bmod 30$

$(-7)^{16} \bmod 30$

$(-7)^{1} \bmod 30 = -7$

$(-7)^{2} \bmod 30 = 19$ or -11

$(-7)^{4} \bmod 30 = ((-7)^{2} \bmod 30 \times (-7)^{2} \bmod 30) \bmod 30$

$= (-11 \times -11) \bmod 30$

$= 121 \bmod 30$

$= 1$

$(-7)^{8} \bmod 30 = ((-7)^{4} \times (-7)^{4}) \bmod 30$

$= 1 \bmod 30$

$(-7)^{16} \bmod 30 = \left((-7)^8 \bmod 30 \times (-7)^8 \bmod 30\right) \bmod 30$

$= (1 \times 1) \bmod 30$

$= 1$

Practice set :-

Find the result of following using fermat's little theorem :-

(1) $5^{15} \bmod 13$

(2) $15^{18} \bmod 17$

(3) $456^{17} \bmod 17$

(4) $145^{102} \bmod 101$

(5) $5^{-1} \bmod 13$

(6) $15^{-1} \bmod 17$

(7) $27^{-1} \bmod 41$

(8) $70^{-1} \bmod 101$

find the result of following using "Euler's theorem".

(1) $12^{-1} \bmod 77$

(2) $16^{-1} \bmod 323$

(3) $20^{-1} \bmod 403$

(4) $44^{-1} \bmod 667$