Unit-3

1) Mathematics of Asymmetric Key

* It is classified into six types they are

* Prime Numbers
* primality Testing
* Factorization
* Euler's Theorem
* Chinese Remainder theorem
* Exponentiation and logorith

Prime Number:

* An integer P > 1
* If its only divisors of 1 and P
* It is also known as fundamental theorem of arthimetic

Primality Testing:

* A primality test is an algorithm used for determining whether the input is prime.

* It is used for cryptography

* primality tests do not generally give prime factors, it states whether the input number is prime or not

* some primality tests prove that a number is prime they are

1) The seive of Erothosthenes

2) prime factorization

Euler's theorem:

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

Consider, $a = 3$ and $n = 10$

$$3^{\phi(10)} = 1 \pmod{10}$$

$$\phi(10) = 4$$

$3^4 = 1 \pmod{10}$

$81 = 1 \pmod{10}$

* The numbers a and n must be prime.

Chinese Remainder theorem:

* The Chinese remainder theorem (CRT) is used to solve a set of different congruent equation with one variable but different moduli which are relatively prime.

* It is a one of most useful results of number theory.

* Let us consider some linear system of congruences

$x = a_1 \pmod{n_1}$

$x = a_2 \pmod{n_2}$

....

$x = a_n \pmod{n_m}$.

*CRT states that the equations have a unique solution of the modulo and that are relatively prime

Eg:

$$x = (a_1 M_1 M_1^{-1} \quad a_2 M_1 M_2^{-1} \ldots + a_n M_n M_n^{-1}) \text{ Mod } M$$

Consider a set of congorent equations

$$x = 2 \pmod 3$$
$$x = 3 \pmod 5$$
$$x = 2 \pmod 7$$

$x = a_1 \pmod{m_1}$	$x = 2 \pmod 3$
$x = a_2 \pmod{m_2}$	$x = 3 \pmod 5$
$x = a_3 \pmod{m_3}$	$x = 2 \pmod 7$

$$x = (a_1 M_1 M_1^{-1} \quad a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \text{ Mod } M$$

Given $a_1 = 2$ $m_1 = 3$

$a_2 = 3$ $m_2 = 5$

$a_3 = 2$ $m_3 = 7$

To find.

M_1 M_1^{-1}

M_2 M_2^{-1} M

M_3 M_3^{-1}

To find $M = m_1 \times m_2 \times m_3$

$M = 3 \times 5 \times 7$

$\boxed{M = 105}$

To find $M_1 = \frac{M}{M_1} = \frac{105}{3} = 35$

To find $M_2 = \frac{M}{M_2} = \frac{105}{5} = 21$

To find $M_3 = \frac{M}{M_3} = \frac{105}{7} = 15$

To find inverse of M

$M_1 \times M_1^{-1} = 1 \mod m_1$

$35 \times M_1^{-1} = 1 \mod 3$

$35 \times 2 = 1 \mod 3$

$M^{-1} = 2$

$M_2 \times M_2^{-1} = 1 \text{ Mod } m_2$

$21 \times M_2^{-1} = 1 \text{ Mod } 5$

$21 \times 1 = 1 \text{ Mod } 5$

$M_2^{-1} = 1$

$M_3 \times M_3^{-1} = 1 \text{ Mod } m_3$

$15 \times M_3^{-1} = 1 \text{ Mod } 7$

$15 \times 1 = 1 \text{ mod } 7$

$M_3^{-1} = 1$

$= (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \text{ Mod } 105$

$= 233 \text{ Mod } 105$

$x = 23 //.$

2) RSA Algorithm:

* The Rivest - Shamir - Adleman (RSA) has invented algorithm for converting plaintext to ciphertext

* The typical size for n is 1024 bits or 309 decimal digits

Algorithm:

* pick two large prime numbers p and Q. such that $P \neq q$

* Calculate $n = P \times Q$

* Calculate $\phi(n) = (P-1) \times (q-1)$

* pick "e". so that $GCD[e, \phi(n)] = 1$

$1 < e < \phi(n)$

* calculate encryption using

$C = M^e \bmod n$

Decryption using

$M = C^d \bmod n$.

Eg:

1) $p = 17$

$q = 11$

$e = 7 \quad M = 88$

2) $n = p \times q$

$n = 17 \times 11$

$n = 187$

3) $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$

4) Encryption

$C = M^e \bmod n$

$= 88^7 \bmod 187$

$= 11$

5) Decryption $M = C^d \bmod n$

$M = 11^{23} \bmod 187$

$= 88$

3) Diffie Hellman Key exchange:

* It is an first published public Key algorithm that defines public Key cryptography.

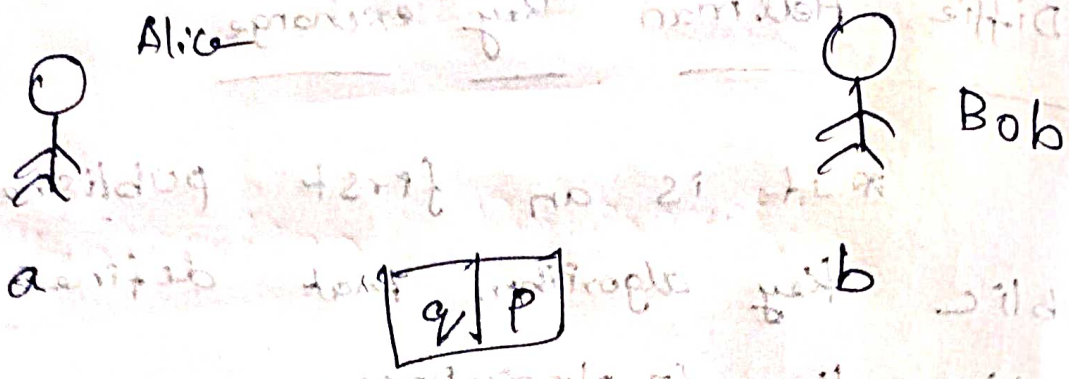
* The main purpose of this algorithm is to enable two users to securely exchange a key that can be used for encryption of Msges.

* This algorithm is limited to exchange of secret values

Why this is secure?

* It is uses discrete logarithm algorithm to avoid forced attack

* It is used for the exchange of private key not public key



a → denotes private value of Alice

b → denotes private value of Bob

q → denotes prime Number

p → It denotes primitive root

$A = p^a \bmod q$

$B = p^b \bmod q$

A ⟶

⟵ B

Alice

Bob

$S = B^a \bmod q$

$S = A^b \bmod q$

Q9:

$q = 13, \quad p = 6$

Alice — Bob

Prive value $a = 3$ — $b = 10$

$A = p^a \bmod q$

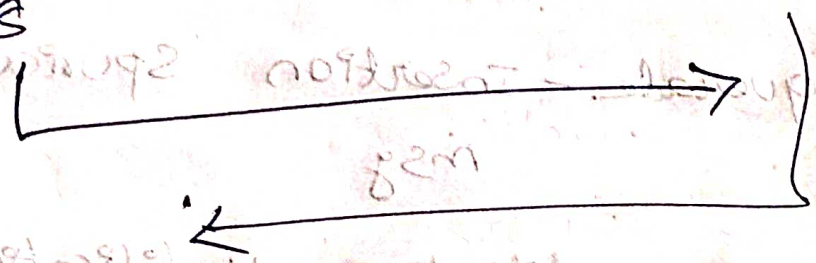
$= 6^3 \bmod 13$

$= 8$

$B = p^b \bmod q$

$= 6^{10} \bmod 13.$

$= 4$



$S = A^b \bmod q$

$S = 8^{10} \bmod 13$

$= 12$

$S = B^a \bmod q$

$= 4^3 \bmod 13$

$= 12$