UNIT- III

Asymmetric Encryption

→ Both encryption and decryption purpose we use different keys.

→ Public key encryption.

→ confidentiality and Authentication.

Mathematics of Asymmetric key cryptography:

primes:

→ Asymmetric key cryptography uses prime numbers extensively.

→ A prime is divisible by itself and 1.

2 4

- positive integers.
  - Number 1 — Exactly one divisor
  - Primes — Exactly two divisors
  - composites — More than two divisors.

Number of primes:

1

$\pi(x)$.

→ That is number of primes $\leq x$.

Ex: $\pi(2) = 1$.

$\pi(3) = 2$. 2, 3.

$\pi(25) = 9$.

Multiplicative Inverse:

→ If 'p' is a prime and 'a' is a integer such that p does not divide 'a' then

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

Ex: How to calculate multiplicative inverse of 5 modulo 23 that is $5^{-1} \bmod 23$?

($a = 5$, $p = 23$)

Sol:

$$5^{-1} \bmod 23 = 5^{23-2} \bmod 23$$

$$5^{-1} \bmod 23 = 5^{21} \bmod 23.$$

$$= (5^{16} \times 5^{4} \times 5^{1}) \bmod 23.$$

$$\boxed{5^{16+4+1}}$$

23) 25 (1
23
2

$(a^m)^n = a^{m \times n}$

$5 \bmod 23 = 5$;

$5^2 \bmod 23 = 25 \bmod 23 = 2$,

$5^4 \bmod 23 = (5^2)^2 \bmod 23 = 2^2 \bmod 23$

$= 4 \bmod 23 = 4.$

$5^8 \bmod 23 = (5^4)^2 \bmod 23 = (4)^2 \bmod 23$

$= 16 \bmod 23 = 16.$

$5^{16} \bmod 23 = (5^8)^2 \bmod 23 = (16)^2 \bmod 23$

$= 256 \bmod 23 = 3,$

$5^{-1} \bmod 23 = (5^{16} \times 5^4 \times 5^1) \bmod 23.$

$= (3 \times 4 \times 5) \bmod 23.$

$= 60 \bmod 23 = 14$

$5^{-1} \bmod 23 = 14.$

Euler's totient function: 23)256(
20

→ Euler's totient function, also known as phi-function $\phi(n)$

→ This function counts number of integers in set.

→ It contains some of the properties,

1. $\phi(1) = 0$ x
2. If P is a prime, then $\phi(P) = P-1$
3. If a & b are relatively prime then $\phi(ab) = \phi(a).\phi(b)$
4. If p is a prime then, $\phi(p^e) = p^e - p^{e-1}$

Relatively prime:

→ Two numbers are said to be relatively prime when they share no factors will common other than 1.

Ex: $a = 15, b = 28.$

$a = 15 = 1 \times 3 \times 5.$

$b = 28 = 1 \times 2 \times 2 \times 7. = 1 \times 4 \times 7$

$= \cancel{1 \times 7 \times 2}$

Ex: Find $\phi(7)$

Sol: $\phi(7) = 7-1 = 6$

2. Find $\phi(21)$

Sol: ~~$\phi(21) = 21-1 = 20$.~~

$\phi(3\times 7) = \phi(3)\times\phi(7) = 3-1 \times 7-1$

$= 2\times 6 = 12$.

3. Find $\phi(3^2) = 3^2 - 3^{2-1}$.

$= 3^2 - 3^1$

$p^e - p^{e-1}$

$= 9-3 = 6$

Fermat's little theorem:

1. If p is a prime number and, a is +ve integer, such that 'p' does not divide 'a', then $a^{p-1} \equiv 1 \bmod p$.
2. $a^p \equiv a \bmod p$.

Ex: Find the result of $6^{10} \bmod 11$

Sol: 1. $6^{11-1} \equiv 1 \bmod 11$

$6^{10} \bmod 11 = 1 \bmod 11$

$6^{10} \equiv 1 \bmod 11$.

$6^{10} \bmod 11 = 1$

2. $6^{11} \equiv 6 \bmod 11$

$6^{11} \bmod 11 = 6 \bmod 11$.

$6^{11} \bmod 11 = 6$.

Chinese Remainder Theorem:

→ It is used to solve a set of congruent equations with 1 variable but different modulo and which are relatively prime, then

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$.

$x \equiv a_3 \pmod{m_3}$.

$\vdots$

$x \equiv a_n \pmod{m_n}$

Solution to Chinese Remainder Theorem.

1. Find $M = m_1 \times m_2 \times \dots \times m_n$.

2. Find $M_1 = M/m_1$,

$M_2 = M/m_2$,

$\vdots$

$M_n = M/m_n$.

3. Find the multiplicative inverse of $M_1, M_2, \dots M_n$ using the corresponding moduli $(m_1, m_2, \dots, m_n)$. Call the inverses $M_1^{-1}, M_2^{-1}, \dots, M_n^{-1}$.

4. The solution is.

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \dots + a_n \times M_n \times M_n^{-1}) \bmod M.$$

1. Find the solution to the simultaneous equations:

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

Sol: 1. $M = 3 \times 5 \times 7 = 105$.

2. $M_1 = 105/3 = 35$.

$M_2 = 105/5 = 21$.

$M_3 = 105/7 = 15$.

$3)\,70\,(23$
$\;\;6\downarrow$
$\;\;10$
$\;\;\;9$
$\;\;\;1$

3. The inverses are $M_1^{-1} = 35^{-1}$

$M_1 \times M_1^{-1} \equiv 1 \bmod m_1$.

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

$35 \times 2 = 1 \bmod 3$.

$M_1^{-1} = 2$.

$M_2 \times M_2^{-1} = 1 \bmod m_2$

$\underline{21 \times M_2^{-1} = 1 \bmod 5}$

$21 \times \underline{1} = \underline{1} \bmod 5$

$M_2^{-1} = \underline{1}$

$5 \overline{)\, 21}\, (4$
$\;\; 20$
$\;\; \overline{\;\; 1}$

• $M_3 \times M_3^{-1} = 1 \bmod m_3$

$15 \times M_3^{-1} = \underline{1} \bmod 7$

$7 \overline{)\, 15}\, (2$
$\;\; 14$
$\;\; \overline{\;\; 1}$

$15 \times 1 = 1 \bmod 7$

$M_3^{-1} = 1$

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

$= (140 + 63 + 30) \bmod 105$

$= \underline{233} \bmod 105$

$105 \overline{)\, 233}\, (2$
$\;\; 210$
$\;\; \overline{\;\; 23}$

$\boxed{x = 23}$

$\underline{23} \equiv 2 \pmod 3$

$3 \overline{)\, 23}\, (7$
$\;\; \overline{21}$
$\;\; 2$

Principles of public key cryptography:

→ The most difficult problems in symmetric Encryption.

a. ~~E~~ key Exchange problem.

b. Trusted problem.

1. RSA Algorithm:

→ RSA stands for Rivest - Shamir and Adleman.

→ This Algorithm is a Asymmetric algorithm with 2 different keys.

Steps for Algorithm:

1. select 2 large prime numbers i.e, P & q.

$\phi(P) = P-1$

2. $n = p * q$.
3. calculate Euler's Totient function.

$$\phi(n) = (p-1)(q-1)$$

4. select the value 'e' and $GCD(e, \phi(n)) = 1$
5. calculate the value of 'd'

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

(or)

$$ed \bmod \phi(n) = 1$$

6. Public key → (e, n).
   private key → (d, n).
7. Encryption

$$c = m^e \bmod n$$

8. decryption

$$m = c^d \bmod n.$$

1. Encrypt plain text '5' using RSA algorithm and prime numbers $P = 3, q = 11$ and to generate public & private keys.

Sol: 1. $p = 3, q = 11$.

2. $n = p * q \Rightarrow 3 * 11 = 33$

3. $\phi(n) = (3-1)(11-1)$ $\quad (P-1)(q-1)$

$= (2)(10)$

$= 20$.

4. $GCD(e, \phi(n)) = 1$

$GCD(e, 20) = 1$.

$GCD(3, 20) = 1$

$e = 3$ $\quad$ 3, 20.

5. $d = e^{-1} \bmod \phi(n)$

$ed \bmod \phi(n) = 1$.

$3 \times d \bmod 20 = 1$.

$3d \bmod 20 = 1$. $\quad$ 1 mod 20,

$3 \times 7 \bmod 20 = 1$. $\quad$ 1, 21

$d = 7$.

6. public key $= (e, n) = (3, 33)$ $\quad$ $20 \overline{)21(1}$, 20, 1

private key $= (d, n) = (7, 33)$.

7. Encryption

$C = 5^3 \bmod 33$. $\quad$ $m^e \bmod n$.

$= 125 \bmod 33$. $\quad$ $m \rightarrow P.T$

$C = 26$. $\quad$ $33 \overline{)125(}$

8. decryption

$m = c^d \bmod n$.

$= 26^7 \bmod 33$.

$m = 5$

Diffie Hellman key Exchange:

→ This algorithm used to exchange cryptography keys over public communication channel. This algorithm sender & receiver can generate same keys that is k_1 and k_2.

$k_1 = B^x \bmod P$, $k_2 = A^y \bmod P$.

steps for Algorithms:

1. select 2 prime numbers i.e, P, q.
2. A can choose another random number x and calculate

   $\boxed{A = q^x \bmod P}$ and send to B.

3. B can choose another random number y and calculate

   $\boxed{B = q^y \bmod P}$ and send to A.

4. calculate A & B keys.

$K_1 = B^x \bmod P$.

$K_2 = A^y \bmod P$.

Ex:

1. $P = 11, q = 7$.

$A = q^x \bmod P$.

$B = q^y \bmod P$.

2. $x = 3$.

$A = 7^3 \bmod 11 = 2$ → sent to B.

P.T →

3. $y = 6$.

$B = 7^6 \bmod 11 = 4$ → sent to A.

4. $A = 2, B = 4$.

$K_1 = 4^3 \bmod 11$

$= 64 \bmod 11$

$\boxed{K_1 = 9}$

11) 64 (5
55
9

$K_2 = 2^6 \bmod 11$

$= 64 \bmod 11$

$\boxed{K_2 = 9.}$

11) 64 (5
55
9

ELGAMAL Crypto System:

→ It is a public key crypto system and uses asymmetric key encryption for communicating between sender and reciever. This algorithm following these steps.

1. key Generation
2. Encryption
3. Decryption.

Key Generate.

select P (Prime)
select $e_1 \to$ Random
select $d \to$ Random
$e_2 = e_1^d \bmod p$

Public key (e_1, e_2, p)

Private key (d)

P.T → $C_1 = e_1^r \bmod P$
$C_2 = (e_2^r \times P.T) \bmod P$

Encryption

C_1, C_2

$P.T = C_2 \times (C_1^d)^{-1} \bmod P$

Decryption

Ex: key generation:

$p = 11$

$e_1 = 2$

$d = 3$

$e_2 = 2^3 \bmod 11 = 8 \bmod 11 = 8$

public key $= (2, 8, 11)$

private key $= (3)$

Encryption:

$P.T = 7$

$r = 4$

$C_1 = 2^4 \bmod 11 = 16 \bmod 11 = 5$

$C_2 = (8^4 \times 7) \bmod 11$

$= 28672 \bmod 11 = 6$

cipher text $= (C_1, C_2) = (5, 6)$

$11 \overline{)16} (1$
11
$\overline{5}$

Decryption:

$C_2 \times (C_1^d)^{-1} \bmod P$

$P.T = 6 \times (5^3)^{-1} \bmod 11$

$\boxed{125 \times x \equiv 1 \bmod 11}$

$= 6 \times (125)^{-1} \bmod 11$

$= 6 \times [(125 \times x) \bmod 11 = 1 \bmod 11]$

$= 6 \times [(125 \times 3) \bmod 11 = 1]$

375

$= 6 \times 3 \bmod 11$

$11 \overline{)375} (34$
33
$\overline{45}$
44
$\overline{1}$

$= 18 \bmod 11$

P.T. $= 7$.

$$\begin{array}{r} 11\overline{)18(1} \\ 11 \\ \hline 7 \end{array}$$