Deffie Hellman key exchange Algorithm:-

Algorithm.

Algorithm:-

1. It is not an encryption (or) decryption
2. It is used to exchange keys b/w sender and reciever.
3. It is Asymmetric key cryptography.

1. Consider the prime number (q)

2. Select α, where "α" is premptive root of q.

$$\boxed{\alpha < q}$$

x - private
y - public.

3. Assume $\rightarrow x_A$ (private key for A) ($x_A < q$)

$$\boxed{Y_A = \alpha^{x_A} \bmod q}$$ (Y_A = Publickey of A)

4. Assume $\rightarrow x_B$ (private key for B) ($x_B < q$)

$$\boxed{Y_B = \alpha^{x_B} \bmod q}$$

5. Calculate Secret key 'k_1' and 'k_2'

$$\boxed{k_1 = (Y_B)^{x_A} \bmod q}$$

$$\boxed{k_2 = (Y_A)^{x_B} \bmod q}$$

$\therefore k_1 = k_2$

Success

key exchanged Successfully.

Primitive Root = ?

$\alpha^1 \bmod q$

$\alpha^2 \bmod q$

$\alpha^3 \bmod q$

$\vdots$

$\alpha^{q-1} \bmod q$ should have value $\{1, 2, 3 \cdots q-1\}$

$q = 11$, $X_A = 8$, $X_B = 4$.

$\alpha = ?$

$\alpha^{q-1} \bmod q$ $\qquad\qquad$ $2^4 \bmod 11$.

$\alpha^{11-1} \bmod q$ $\qquad\qquad$ $2 \times 2 \times 2 \times 2 \times 2 \bmod 11$

$\alpha^{10} \bmod q$ $\qquad\qquad$ $2^5 \bmod 11$ $\qquad$ $11 \overline{)32} (2$, 22, 10

	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3										
4										
5										
6										
7										

$\boxed{\alpha = 2}$

$X_A = 8$

$Y_A = \alpha^{X_A} \bmod q$

$Y_A = 2^8 \bmod 11$

$\boxed{Y_A = 3}$

$X_B = 4$

$Y_B = \alpha^{X_B} \bmod q$

$= 2^4 \bmod 11$

$\boxed{Y_B = 5}$

$k_1 = Y_B^{X_A} \bmod q$

$= 5^8 \bmod 11$

$\boxed{= 4}$

$k_2 = (Y_A)^{X_B} \bmod q$

$= (3)^4 \bmod 11$

$\boxed{= 4}$

$\boxed{k_1 = k_2}$

key exchange successful.

Eulers totiem function

If n is prime $\rightarrow \phi(n) = (n-1)$

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

p and q are primes

$n = a \times b$ $\rightarrow \phi(n) = n \times \left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)$

Eiether a or b is composite

Both a & b is composite

where P_1, P_2 are distinct primes

Ex:

$n = 5$

n is a prime

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

$\phi(5) = (5-1)$

$\boxed{\phi(5) = 4}$

$n = 31$

n is prime

$\phi(31) = (31-1)$

$\boxed{\phi(31) = 30}$

$n = 35$

n is a product of 2 primes 5 & 7

$\phi(n) = (5-1)(7-1)$

$\phi(n) = (4)(6)$

$\boxed{\phi(n) = 24}$

④ Find $\phi(1000)$

$n = 1000$

$n = 2^3 \times 5^3$

Distinct primes factors 2 & 5

$\phi(n) = n \times \left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)$

$= 1000 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$

$= 1000 \times \left(\frac{2-1}{2}\right)\left(\frac{5-1}{5}\right)$

$= \cancel{1000}^{\cancel{200}\ 100} \times (1/2)(4/\cancel{5})$

$= 100 \times 4$

$= 400$

Fermats little theorem:

If p is a PN and a is a +ve integer not divisible by p then $a^{p-1} \equiv 1 \pmod{p}$

Ex: Does hold true $p=5$ & $a=2$

Given: $p=5$

$a=2$

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

$2^4 = 1 \pmod{5}$

$16 = 1 \pmod{5}$

Given $p=13$

$a=11$

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

$11^{12} = 1 \pmod{13}$

$-2^{12} = 1 \pmod{13}$

$-2^{4\times3} = 1 \pmod{13}$

$3^3 = 1 \pmod{13}$

$27 = 1 \bmod 13$

$\boxed{\text{Holds true}}$

$p=6$

$a=2$

$2^5 = 1 \pmod{6}$

$32 = 1 \pmod{6}$

(5) $p = 11$

$a = 5$

$5^{11-1} = 1 \pmod{11}$

$5^{10} = 1 \pmod{11}$

$5^{2\times5} = 1 \pmod{11}$

$3^5 = 1 \pmod{11}$

$243 = 1 \pmod{11}$

Holds true ✓

$81 \times 3 = 243$

$11) 243 (22$
22
23
22
1

Euler's theorem:

For every +ve integer a & n which are said to be relatively prime then

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

Ex: $a = 3$

$n = 10$

$a^4 = 1 \bmod n$

$3^4 = 1 \bmod 10$

$81 = 1 \bmod 10$

~~1 = 1 mod 10~~

holds (✓)

$a = 2$

$n = 10$

$2^4 = 1 \bmod 10$

$16 = 1 \bmod 10$

not holds (✗)

ex: $a = 10$

$n = 11$

$a^{10} \equiv 1 \mod n$

$10^{10} \equiv 1 \mod 11$

$\therefore 1^{2 \times 5} = 1 \mod 11$

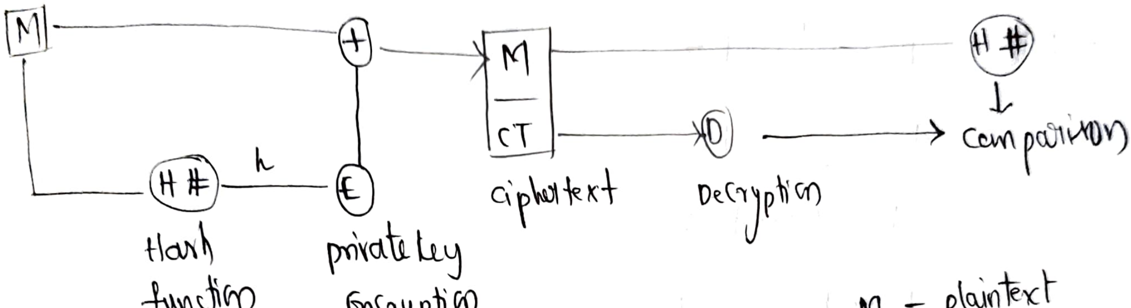
$1 = 1 \mod 11$

Holds true (✓)

unit-3

RSA Algorithm

- Rivest - shamir - Adleman Algo
- Along with signature verification, it can be used for encryption and decryption of standard data.
- Below figure is a process of verifying signatures using RSA



M - plaintext
h - digest

- RSA is Asymmetric key and Block Cipher Algo
- it has 3 steps

1. Key Generation
2. Encryption
3. Decryption

Steps

1. Select 2 large prime numbers p and q

2. compute $n = q * p$ and

$z = (p-1)(q-1)$

3. choose a number e

where $1 < e < (p-1)(q-1)$

4. Calculate $d = e^{-1} \bmod z$

$d = \frac{1}{e} \bmod z$

$ed = 1 \bmod z$

$ed \bmod z = 1$

5. public key $= \{e, n\}$

private key $= \{d, n\}$

6. Encryption

$c = m^e \bmod n$

m = no. of digits in PT (Assume) $\boxed{m<n}$

c = cipher text

7. Decryption

$m = c^d \bmod n$

Example

1. $p = 3 \qquad q = 11$

2. $n = p * q = 3 * 11$

$= 33$

$z = (3-1)(11-1)$

$= 2(10)$

$= 20$

3. chose $e \qquad 1 < e < z$

$\gcd(7, 20) = 1$ (take)

$\boxed{e = 7}$

4. $ed \bmod z = 1 \qquad d = ?$

$7(1) \bmod 20 = 13$ ✗

$7(2) \bmod 20 = 6$ ✗

$7(3) \bmod 20 = 1$ ✓

$\boxed{d = 3}$

5. public key $\rightarrow \{e, n\} = \{7, 33\}$

private key $\rightarrow \{d, n\} = \{3, 33\}$

6. Encryption

$c = m^e \bmod n$ $\qquad \boxed{m < n} \rightarrow$ take any number that is less than n

$= (31)^7 \bmod 33$ $\qquad$ let $\boxed{m = 31}$

$\boxed{c = 4}$

7. Decryption

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

$$= (4)^3 \bmod 33$$

$$= 64 \bmod 33$$

$$\boxed{m = 31}$$