UNIT-III

Mathematical asymmetric key Cryptography
Asymmetric key Cryptography

Asymmetric Encryption:-

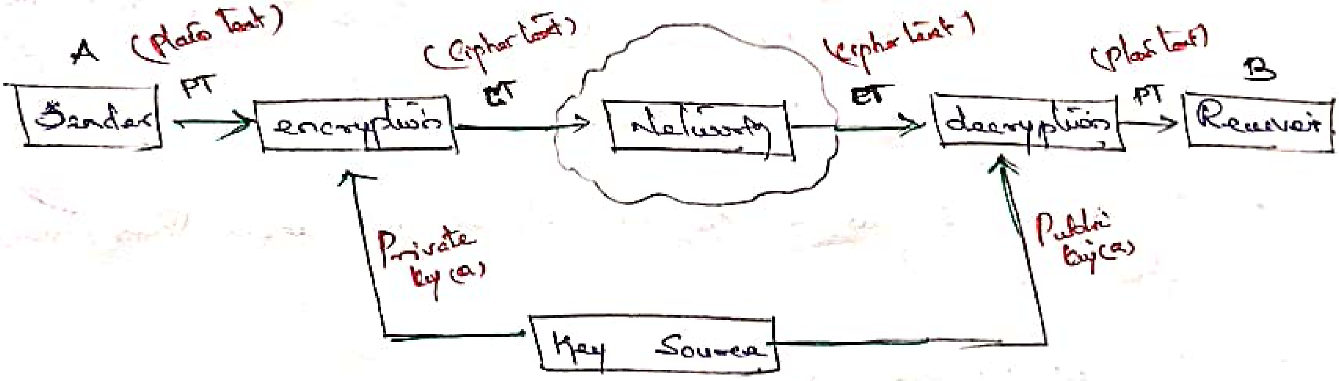
PRINCIPLES OF PUBLIC KEY CRYPTOSYSTEMS:-

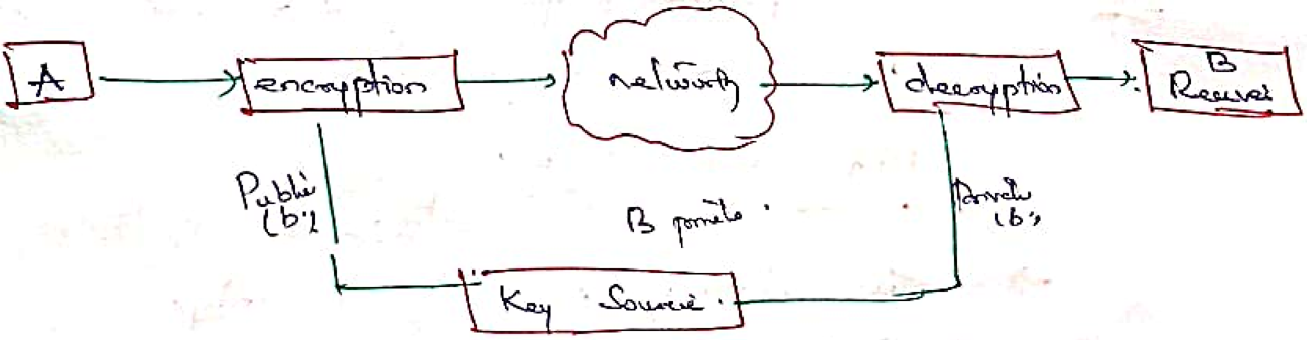
(Asymmetric Key Cryptography)

There are two principles.

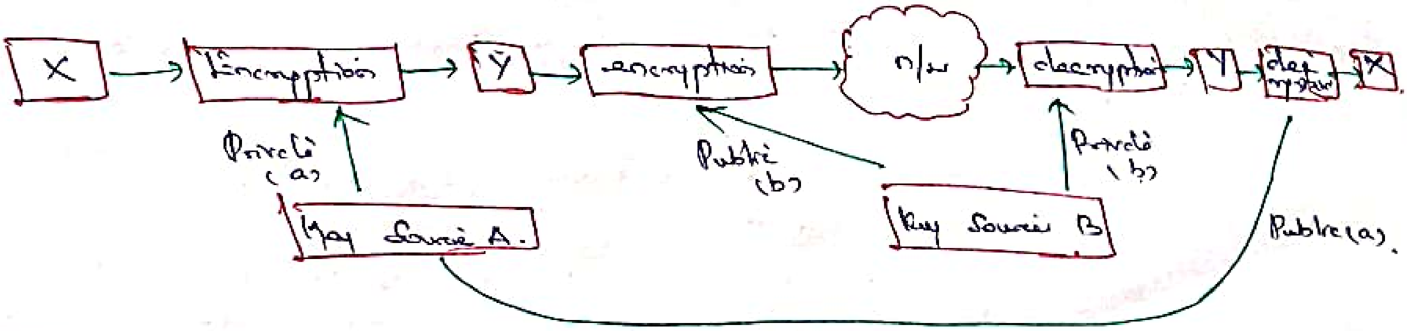
1. Authentication
2. Confidentiality

Authentication:-



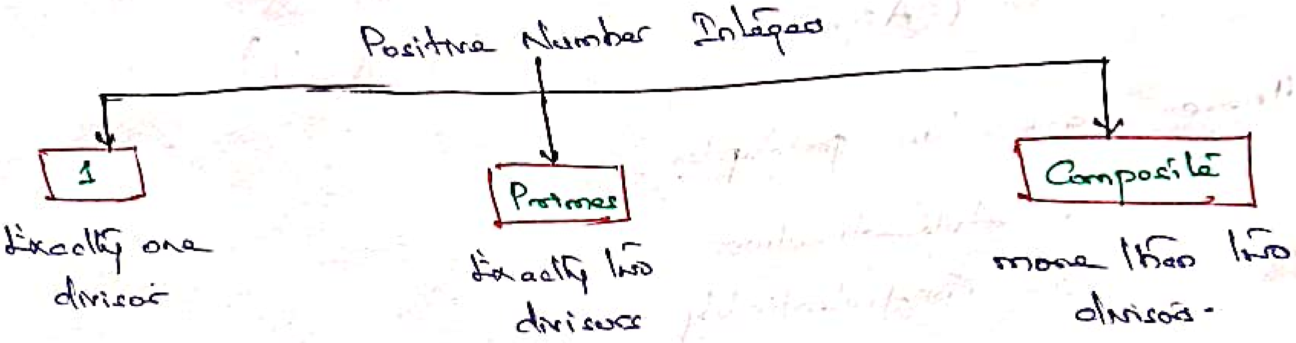


Confidentiality:-



Primes:-

★ Asymmetric key Cryptography Uses primes extensively.



★ A positive integer is a prime if and only if it is exactly divisible by two integers,

ie:- 1 or itself.

★ A Composite is a positive integer will more than two divisors.

★ Smallest prime is: 2.

★ Coprime:- Two positive integers a and b are relatively prime or Coprime.

$\boxed{\text{if } \gcd(a,b) = 1 .}$

⇒ 1 is relatively prime to any integers

⇒ if 'p' is prime number, then all integers 1 to p-1 are relatively prime to 'p'

Smallest prime:-

Smallest prime is 2, which is divisible by 2 (itself) and 1.

List the prime Smaller than 10.

There are four primes less than 10,

2, 3, 5 and 5

The percentage of primes in the range 1 to 10 is 40%.

The percentage decreases as the range increase.

Asymmetric : exponent
Multiplicative function

Euler's Theorem:

If $\underline{a}$ and $\underline{n}$ are relatively prime, then

$$\boxed{\gcd(a,n) = 1}$$

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

$\equiv$ Congruent to [illegible]

$\phi(n)$ - number of positive integers less than n & relatively prime to n.

Example:-

$a = 6 \quad n = 11 \quad \gcd(6,11) = 1 \quad \phi(11) = \overset{n-1}{11-1} = 10$

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

$6^{\phi(11)} \equiv 1 \pmod{11} \Rightarrow 6^{10} \equiv 1 \pmod{11}$

$\boxed{6^{10} \bmod 11 = 1}$ ← Sit true or false.

$6^2 \bmod 11 \Rightarrow 36 \bmod 11 \Rightarrow 3$

$6^4 \bmod 11 \Rightarrow (6^2)^2 \bmod 11 \Rightarrow 3^2 \bmod 11 \Rightarrow 9 \bmod 11 = 9$

$6^8 \bmod 11 \Rightarrow (6^4)^2 \bmod 11 \Rightarrow (9)^2 \bmod 11 \Rightarrow 81 \bmod 11 \Rightarrow 4$

$6^{10} \bmod 11 \Rightarrow (6^8) \bmod 11 \cdot 6^2 \bmod 11 \Rightarrow 4 \times 3 \bmod 11$

$\Rightarrow 12 \bmod 11$

$= 1$ Hence proved.

(or) $\boxed{6^{10} \bmod 11 = 1}$

$6^2 \bmod 11 \Rightarrow 36 \bmod 11$

$\Rightarrow 3$

$$\begin{array}{r|l} & 3 \\ \hline 11 & 36 \\ & 33 \\ \hline & 3 \end{array}$$

$6^4 \bmod 11 \Rightarrow (6^2)^2 \bmod 11$

$\Rightarrow 3^2 \bmod 11$

$\Rightarrow 9 \bmod 11$

$= 9$

$$\begin{array}{r|l} & 2 \\ \hline 11 & 27 \\ & 22 \\ \hline & 5 \end{array}$$

$6^6 \bmod 11 \Rightarrow$ Too lengthy / $(6^2)^3 \bmod 11 \Rightarrow 3^3 \bmod 11$

$\Rightarrow 27 \bmod 11$

$\Rightarrow 5$

$6^8 \bmod 11 \Rightarrow (6^4)^2 \bmod 11$

$= 9^2 \bmod 11$

$= 81 \bmod 11$

$= 4$

$$\begin{array}{r|l} & 7 \\ \hline 11 & 81 \\ & 77 \\ \hline & 4 \end{array}$$

$6^{10} \bmod 11 \Rightarrow (6^2)^5 \bmod 11$

$= 3^5 \bmod 11$

$= 243 \bmod 11$

$$\begin{array}{r|l} & 22 \\ \hline 11 & 243 \\ & 22 \\ \hline & 23 \\ & 22 \\ \hline & 1 \end{array}$$

$\boxed{6^{10} \bmod 11 = 1}$ Hence solved.

Practice:

$a = 8 \quad n = 13 \quad \gcd(8,13) = 1$ ✓
$a = 5 \quad n = 17$ ✓
$a = 4 \quad n = 12$ ✗
$a = 3 \quad n = 23$ ✓
$a = 3, \quad n = 17$

Eulers Totient Function :-

Guwei

It is defined as the number of positive integer less than and relatively prime to n, It is denoted by $\phi(n)$

$n=3$ 1, 2 $\gcd(1,3) \rightarrow 1 \rightarrow RP$

$\gcd(2,3) \rightarrow 2 \rightarrow R \rightarrow P$

(i) If n is prime $\phi(n) \Rightarrow n-1$ $n=3 \rightarrow n-1 = \boxed{2}$.

(ii) If n is not prime

n is not prime

3 Cases

ⓐ $\phi(n) \rightarrow n = p \cdot q$ $\phi(p \cdot q) \Rightarrow \phi(p) \cdot \phi(q)$

$\Rightarrow (p-1)(q-1)$

$\phi(6) \Rightarrow 2 \times 3$ $\phi(2 \cdot 3) \Rightarrow \phi(2) \cdot \phi(3)$

1, 2, 3, 4, 5 $= (2-1)(3-1)$

$\gcd(1,6) \Rightarrow 1$ ✓ $= 1 \cdot 2 = \boxed{2}$

$\gcd(2,6) \Rightarrow 2$ ✗

$\gcd(3,6) \Rightarrow 3$ ✗

$\gcd(4,6) \Rightarrow 2$ ✗

$\gcd(5,6) \Rightarrow 1$ ✓

$6 \times \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{3}\right)$

$\cancel{6}^{2} \times \frac{1}{2} \times \frac{2}{3}$

$= 2$ //

ⓑ $\phi(n) = \phi(p^i) = p^i - p^{i-1}$

$n = 343 \Rightarrow \phi(7^3) = 7^3 - 7^{3-1} \Rightarrow 343 - 49 \Rightarrow 294$

ⓒ $\phi(n) \Rightarrow n \times \pi\left(1-\frac{1}{n}\right) \Rightarrow n = 42 \Rightarrow 2, 3, 7$

Primes

$= 42 \times \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{3}\right) \times \left(1-\frac{1}{7}\right)$

$= \cancel{42}^{6} \times \frac{1}{\cancel{2}} \times \frac{\cancel{2}}{\cancel{3}} \times \frac{\cancel{6}^{2}}{\cancel{7}}$

$\boxed{\phi(n) = 12}$

Finally the function finds the number of integers that are both smaller than 'n', and these are relatively prime to 'n'

The $\phi(n)$ calculates the number of elements in Z_n^*.

FERMAT'S THEOREM :

If p is prime and a is a positive Integer not divisible by p, then

a [illegible] p [illegible] divide
[illegible] [illegible]

$a \overline{| p} \times$

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

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

1. 'p' is a prime number
2. 'a' is any +ve integer
3. a does not divide p, p does not divide a
4. $a^{p-1} \equiv 1 \bmod p$

$p = 19$ $a = 3$

$$3^{19-1} \equiv 1 \pmod{19}$$

$$3^{18} \equiv 1 \pmod{19}$$

$19 \overline{| 27}$ 1
19
8

$3^{18} \bmod 19 = 1 = ?$

$3^{3} \bmod 19 = 27 \bmod 19$
$= 8$

$3^{18} = (3^3)^6$
$= 8^6 \bmod 19$
$= (8^2)^3 \bmod 19$

$19 \overline{| 64}$ 3
57
7

$$\boxed{\begin{aligned} 8^2 \bmod 19 &= 64 \pmod{19} \\ &= 7 \end{aligned}}$$

$(8^2)^3 \bmod 19 = 7^3 \pmod{19}$
$= (7^2 \bmod 19) \cdot (7 \bmod 19)$
$= 11 \bmod 19 \cdot 7 \bmod 19$
$= (11 \times 7) \bmod 19$
$= 77 \pmod{19}$

$19 \overline{| 49}$ 2
38
11

$19 \overline{| 77}$ 4
76
1

$$\boxed{3^{18} \bmod 19 \Rightarrow 1}$$

Practice:-

1. Find 7^{307} mod 23 Using FT ?
2.

DIFFIE

Al

Problems on FERMAT's THEOREM :-

1. Using Fermat's Theorem, Find $5^{301} \pmod{11}$

$a \quad p$

Sol:

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{if } \gcd(a,p) = 1 \text{, when } p \text{ is prime}$$

$\gcd(a,p) = 1$

$\gcd(5,11) \Rightarrow 1 \qquad p = 11 \leftarrow$ if This Condition holds then apply Fermat's Theorem.

$a = 5 \qquad p = 11$

From Thm:

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

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

$\Rightarrow 5^{10} \bmod 11 = 1$

Qn's

$4^{94} \bmod 13 = ?$

$7^{501} \bmod 13 = ?$

&

$2^{103} \bmod 17 = ?$

$9^{2025} \bmod 11 = ?$

Now:

$5^{301} \bmod 11 \Rightarrow [5^{10}]^{30} \cdot 5^1 \pmod{11}$

$\Rightarrow [5^{10}]^{30} \bmod 11 \cdot 5^1 \bmod 11$

$= 1^{30} \bmod 11 \cdot 5^1 \bmod 11$

$= 1 \pmod{11} \cdot 5 \pmod{11}$

$= 1 \cdot 5 \bmod 11$

$= 5$

$\boxed{\therefore 5^{301} \bmod 11 \Rightarrow 5}$

2. Find $3^{201} \bmod 7$ Using Fermat's Theorem?

$a \qquad p$

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

$\gcd(a,p) = 1$

$\gcd(3,7) \Rightarrow 1$

$a = 3 \qquad p = 7$

From Thm:

$3^{7-1} \equiv 1 \pmod{7}$

$\therefore 3^6 \bmod 7 = 1$

$$\begin{array}{r} 33 \\ 6 \overline{)201} \\ 18 \\ \hline 21 \\ 18 \\ \hline 3 \end{array} \qquad \begin{array}{r} 33 \times 6 \\ \hline 198 \\ 3 \\ \hline 201 \end{array} \qquad \begin{array}{r} 3 \\ 7 \overline{)27} \\ 21 \\ \hline 6 \end{array}$$

$3^{201} \bmod 7 \Rightarrow (3^6)^{33} \bmod 7 \cdot (3^3)^1 \bmod 7$

$\Rightarrow 1^{33} \bmod 7 \cdot 27 \bmod 7.$

$\Rightarrow 1 \cdot 6 \bmod 7 = 6//$

$\boxed{\therefore 3^{201} \bmod 7 = 6}$

DIFFIE HELLMAN KEY EXCHANGE ALGORITHM :

Algorithm:-

Let q be a prime number

Given α, where $\alpha < q$ and

α is primitive root of q

1. It is Not an encryption/ Decryption algorithm
2. It is Used to exchange keys between Sender and Receiver
2. It is an Asymmetric Key Cryptography
4. Encryption involves both private and public key.

USER 'A' KEY GENERATION:

Select Private Key X_A : where $X_A < q$

Calculate Public Key Y_A : $Y_A = \alpha^{X_A} \bmod q$

USER 'B' KEY GENERATION:-

Select Private Key X_B : where $X_B < q$

Calculate Public Key Y_B : $Y_B = \alpha^{X_B} \bmod q$

Primitive root:-

-) Assume a is a primitive root of p

-) If $a \bmod p$, $a^2 \bmod p$, $a^3 \bmod p$, ⋮ $a^{p-1} \bmod p$ which results in 1, 2, 3, ... p-1 the values should not be repeated.

GENERATION OF SECRET KEY BY USER 'A':

$$K_1 = (Y_B)^{X_A} \bmod q$$

GENERATION OF SECRET KEY BY USER 'B':

$$K_2 = (Y_A)^{X_B} \bmod q$$

$\boxed{K_1 = K_2}$ then Key exchange Success.

Now:

$q = 7 \quad \alpha = 3$

3 is primitive of 7 ?

$\equiv$ Congruent

$\phi(q) = \phi(7) \Rightarrow 6 \Rightarrow 2, 3$ Prime factors

$$\alpha^{\frac{\phi(7)}{2}} \bmod 7 \not\equiv 1$$

$$\alpha^{\frac{\phi(7)}{3}} \bmod 7 \not\equiv 1$$

$\not\equiv$ Not Congruent

$$3^{6/2} \bmod 7 \Rightarrow 3^3 \bmod 7 \Rightarrow 27 \bmod 7 \Rightarrow 6 \neq 1$$

$$3^{6/3} \bmod 7 \Rightarrow 3^2 \bmod 7 \Rightarrow 9 \bmod 7 \Rightarrow 2 \neq 1$$

User 'A' Key Generation:-

$X_A = 3 < q = 7$

$Y_A = \alpha^{X_A} \bmod q = 3^3 \bmod 7 = 6$ //

$\left(\begin{matrix} X_A & Y_A \\ 3, & 6 \end{matrix}\right)$

$\boxed{Y_A = 6}$

$$\begin{array}{r|l} 7 & 27 \; (3 \\ & 21 \\ \hline & 6 \end{array}$$

User 'B' Key Generation :-

$$X_B = 4 < q = 7$$

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

$$= 3^4 \bmod 7$$

$$\begin{array}{r} 11 \\ 7\,\overline{)\,81} \\ 7 \\ \hline 11 \\ 7 \\ \hline 4 \end{array}$$

$$\boxed{Y_B = 4}$$

$$\begin{array}{cc} X_B & Y_B \\ (4 & 4) \end{array}$$

Generation of Secret key by User 'A' and Generation of Secret key by User 'B' are equall or Same, then the Conclusion of the key exchange is success.

Finally

$$K_1 = (Y_B)^{X_A} \bmod q$$

$$= 4^3 \bmod 7$$

$$= 64 \bmod 7$$

$$\begin{array}{r} 9 \\ 7\,\overline{)\,64} \\ 63 \\ \hline 1 \end{array}$$

$$\boxed{K_1 = 1}$$

$$K_2 = (Y_A)^{X_B} \bmod q$$

$$= 6^4 \bmod 7$$

$$\begin{array}{r} 5 \\ 7\,\overline{)\,36} \\ 35 \\ \hline 1 \end{array}$$

$$= (6^2 \bmod 7)^2$$

$$= 1^2$$

$$\boxed{K_2 = 1}$$

Now the Generation of Secret key by User 'A' and User 'B' are Same.

$$\boxed{K_1 = K_2}$$

∴ The key exchange Successful:

=*=

V.V.I.

RSA Algorithm :-

Rivest Shamir Adleman

< Public
  Private

1979

ALGORITHM:

$p=17$ $q=11$

1. Select p, q where p and q are prime and $p \neq q$

2. Calculate $n = p * q$

3. Calculate $\phi(n) = (p-1) \cdot (q-1)$

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

4. Select integer e, such that $\gcd(\phi(n), e) = 1$
$1 < e < \phi(n)$

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

Public Key $PU = \{e, n\}$

Private Key $PR = \{d, n\}$

ENCRYPTION by USER A WITH USER B's PUBLIC KEY

Plain text : $M < n$

$\therefore \boxed{C = M^e \bmod n}$

[illegible]
$C = P^e \bmod n$
$P = C^d \bmod n$

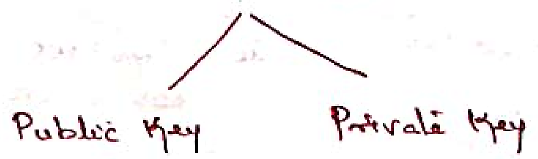
DECRYPTION by USER B WITH USER B's PRIVATE KEY

Cipher text : C

$\boxed{M = C^d \bmod n}$

Extended Euclidean algorithm

Public Key Crypto system



Encryption: → encode into a form such that only authorized users can understand.

Decryption: → Encrypted message → Original form.

Qn: $p = 5$ $q = 31$ $e = 13$ $M = 5$ from the given Valu

we Can Solve RSA Algorithm : ?

As Per the steps in RSA :

Now:

Step:2, $n = p \times q$

$= 5 \times 31$

$\boxed{n = 155}$

Step:3 : Eulers Totient function :

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

$= (5-1) \times (31-1)$

$= 4 \times 30$

$\boxed{\phi(n) = 120}$

Step:4:

$\gcd(120, 13) = 1$

Step:5:-

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

$d = 13^{-1} \bmod 120$

$\boxed{13 \times d \bmod 120 = 1}$

$481 \bmod 120 = 1$

$\boxed{\therefore \quad d = 37}$

d
↓
$13 \times 7 = 91 \bmod 120$
$13 \times 17 = 221 \bmod 120$
$13 \times 27 = 351 \bmod 120$
$13 \times 37 = 481$ ✓

$$\begin{array}{r|l} & 4 \\ \hline 120 & 481 \\ & 480 \\ \hline & 1 \end{array}$$

Extended Euclidean algorithm also used to find d Value.

Now to perform Encryption and Decryption:

Encryption:-

$C = M^{e} \bmod n$

$= 5^{13} \bmod 155$

$= (5^{4})^{3} \cdot 5^{1} \bmod 155$

$= 5^{3} \cdot 5 \bmod 155$

$= 5^{3+1} \bmod 155$

$= 5^{4} \bmod 155$

$= 625 \bmod 155$

$\boxed{C = 5}$

$5^{2} = 25 \bmod 155$ ✗
$5^{3} = 125 \bmod 155$ ✗
$5^{4} = 625 \bmod 155$ ✓

$$\begin{array}{r|l} & 4 \\ \hline 155 & 625 \\ & 620 \\ \hline & 5 \end{array}$$

ie: $5^{4} \bmod 155$
$= 625 \bmod 155$
$= 5$

ie: $5^{13} \bmod 155 = 5$

Decryption :-

$$M = C^d \bmod n$$

$$= 5^{37} \bmod 155$$

$$= (5^{13})^2 \cdot (5^4)^2 \cdot 5^3 \bmod 155$$

$$= (5)^2 \cdot (5)^2 \cdot 5^3 \bmod 155$$

$$= 5^4 \cdot 5^3 \bmod 155$$

$$= 5 \cdot 5^3 \bmod 155$$

$$= 5^4 \bmod 155$$

$$\boxed{M = 5}$$

ie:- $5^{37} \bmod 155 = 5$

We know

$\leftarrow \begin{cases} 5^{13} \bmod 155 = 5 \\ 5^4 \bmod 155 = 5 \end{cases}$

$(5^{13})^2 = 5^{26}$

$(5^4)^2 = 5^8$

$5^3 = 5^3$

$\Rightarrow 5^{26} \cdot 5^8 \cdot 5^3$

$= 5^{26+8+3}$

$\boxed{= 5^{37}}$

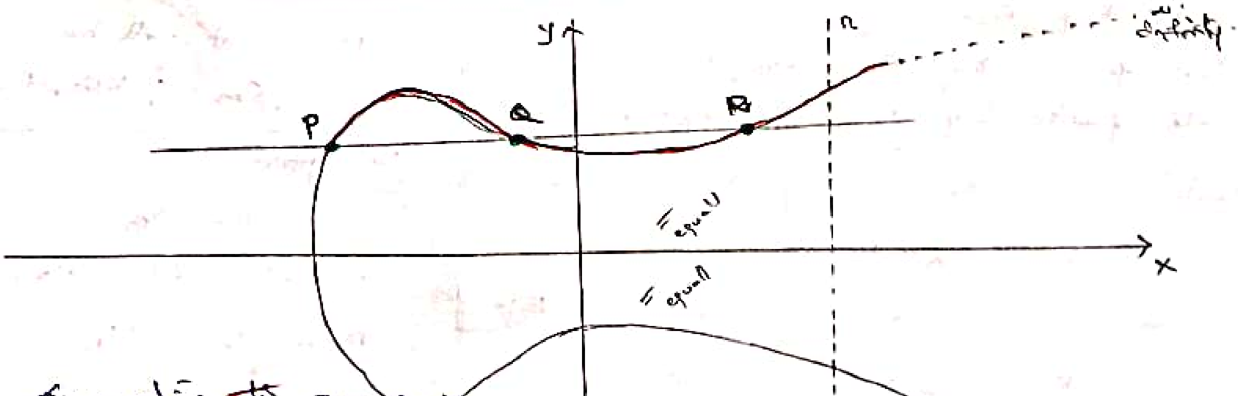
Elliptic Curve Cryptography: (ECC)

- ★ It is asymetric public key cryptography.
- ★ It provides epual Security with Smaller key size (as Compared to RSA) as Compared to non-ECC algorithms

  ie:- Small key size and high security

- ★ It makes Use of Elliptic Curves.
- ★ Elliptic Curves are defined by some mathematical functions- Cubic functions

Eg: $\boxed{y^2 = x^3 + ax + b}$ // epuation of degree 3.



We are limiting it ......

- ★ Symmetric to x-axis
- ★ If we draw a line, it will touch a max of 3 points.

Big Exponential Numbers:-

Default Values

Qn: $\underset{b}{11}^{\overset{e}{6}} \bmod \underset{m}{187}$

$e=6$	$m=187$
$b=11$	$c=1$ (initial) (Constant)

$e'=1$ $\quad c = (b*c) \bmod m = (11\times1) \bmod 187 = 11$

$e'=2$ $\quad c = (b*c) \bmod m = (11\times11) \bmod 187 = 121$

$e'=3$ $\quad c = (b*c) \bmod m = (11\times121) \bmod 187 = 22$

$e'=4$ $\quad c = (b*c) \bmod m = (11\times22) \bmod 187 = 55$

$e'=5$ $\quad c = (b*c) \bmod m = (11\times55) \bmod 187 = 44$

$e'=6$ $\quad c = (b*c) \bmod m = (11\times44) \bmod 187 = \boxed{110}$ //.

Finally

$$\boxed{11^6 \bmod 187 = 110}$$

Thus is the required result.

(or)

$11^6 \bmod 187$ is $\quad 11^2 \bmod 187 = 121 \bmod 187$

$= 121$

$11^4 \bmod 187 = (11^2)^2 \bmod 187$

$= (121)^2 \bmod 187$

$= 14641 \bmod 187$

$= 55$

$= 11^4 \bmod 187 \cdot 11^2 \bmod 187$

$= 11^4 \cdot 11^2 \bmod 187$

$= (121\times55) \bmod 187$

$= 6655 \bmod 187$

$$\boxed{11^6 \bmod 187 = 110}$$ //

Problem on RSA:-

Qn:) $p = 17$, $q = 11$ $m = 88$ from the given e.d. given Values, we can solve the RSA Algorithm ?

Step:1: If $p=17$ and $q=11$ are prime numbers and also $p \neq q$ so the condition satisfied, we can proceed to the next step 2. i.e. $17 \neq 11$

Step:2

$n = p \times q$

$= 17 \times 11$

$\boxed{n = 187}$

Step:3

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

$= (17-1) \times (11-1)$

$= 16 \times 10$

$\boxed{\phi(n) = 160}$

Step:4

$\gcd(e, 160) = 1$, $1 < e < \phi(n)$.

$1 < \overset{}{7} < 160$
$\uparrow$
e

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

$d = 7^{-1} \bmod 160$

$7 \times d \bmod 160 = 1$
$\uparrow$
23

$7 \times 23 \bmod 160 = 1$

$161 \bmod 160 = 1$

$$\begin{array}{r|l} & 1 \\ 160 & 161 \\ & 160 \\ \hline & 1. \end{array}$$

$\boxed{\therefore\ d = 23}$

Now to perform Encryption and Decryption:-

Encryption:-

$d = 23$
$M = 88$
$e = 7$
$n = 187$

$C = M^e \bmod n$

$= 88^7 \bmod 187$

$= (88^4)(88^2) \cdot 88 \bmod 187.$

$= 132 \times 77 \times 88 \bmod 187$

$\boxed{C = 11}$

$88^1 = 88 \bmod 187$
$= 88$
$88^2 = 88^2 \bmod 187$
$= 7744 \bmod 187$
$= 77$
$88^4 = (88^2)^2 \bmod 187$
$= 77^2 \bmod 187$
$= 5929 \bmod 187$
$= 132$

Decryption:-

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

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

$$= (11^{16}).(11^4).(11^2).11^1 \bmod 187$$

$$= 154 \times 55 \times 121 \times 11 \bmod 187$$

$$= 11,273,570 \bmod 187$$

$$\boxed{M = 88}$$

$$\begin{array}{r} 11273570 \\ 11273482 \\ \hline 88 \end{array}$$

$11^1 = 11 \bmod 187$

$= 11$

$11^2 = 121 \bmod 187$

$= 121$

$11^4 = 14641 \bmod 187$

$= 55$

$11^8 = (11^4)^2 \bmod 187$

$= 55^2 \bmod 187$

$= 3025 \bmod 187$

$= 33$

$11^{16} = (11^8)^2 \bmod 187$

$= 33^2 \bmod 187$

$=$

$= 154$

RSA Algorithm:-

① Select p, q , p and q both prime , $p \neq q$.

② Calculate $n = p \times q$

③ Calculate $\phi(n) = (p-1)(q-1)$

④ Select Integer e

$$\gcd(\phi(n), e) = 1; \quad 1 < e < \phi(n)$$

⑤ Calculate d

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

⑥ Public Key

$$PU = \{e, n\}$$

⑦ Private Key

$$PR = \{d, n\}$$

$p = 17 \qquad q = 11$

$n = 17 \times 11 = 187$

$$\begin{aligned}\phi(n) = \phi(pq) &= \phi(p)\phi(q) \\ &= (p-1)(q-1) \\ &= 16 \times 10 \\ &= 160\end{aligned}$$

$e = 7$ ✓ or $e = 11$; $e = 13$ choose any

$d = 7^{-1} \text{ mod } 160 \quad \frac{1}{7} \text{ mod } 160$

$(n \times 7) \text{ mod } 160$

$= 23$

$\boxed{\text{ie } n = 23}$

$(23 \times 7) \text{ mod } 160$

$161 \text{ mod } 160$

$\equiv 1$

$PU = \{7, 187\}$

$PR = \{23, 187\}$

Encryption and Decryption:-

$PU \rightarrow \langle 7, 187 \rangle$

$PR \rightarrow \langle 23, 187 \rangle$

Encryption:-

plain → 2 digit decimal	
plaintext	$M < n \quad 187$
Ciphertext	$C = M^e \text{ mod } n$

$M = 88$

$$\begin{aligned}C &= M^e \text{mod } n \\ &= 88^7 \text{ mod } 187 \\ &= 11\end{aligned}$$

Decryption:-

Cipher text	C
plain text	$M = C^d \text{ mod } n$

Now,

$$\begin{aligned}M &= c^d \text{ mod } n \\ &= 11^{23} \text{ mod } 187 \\ &= 88\end{aligned}$$

Qn: Perform encryption and decryption Using RSA algorithm.

$p=3$; $q=7$, $e=5$; $M=10$ | $P=7$; $q=17$, $e=11$; $M=11$ | $P=17$; $q=23$, $e=9$; $M=7$

$p=5$; $q=13$; $e=5$; $M=8$ | $P=7$; $q=13$, $e=11$; $M=2$

Qn: $P = 13$ $q = 17$

Sln: Step 1: $p=13$ $q=17$

Step 2: $n = 13 \times 17 = 221$

$\boxed{n = 221}$

Step 3: $\phi(n) = 12 \times 16$

$\boxed{\phi(n) = 192}$

Step 4:- $\boxed{e = 35}$

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

$= 35^{-1} \bmod 192$

$= \frac{1}{35} \bmod 192$

$\boxed{d = 11}$

$0 \times 35 \bmod 192 = 0$

$1 \times 35 \bmod 192 = 35$

$2 \times 35 \bmod 192 = 70$

$3 \times 35 \bmod 192 = 105$

$4 \times 35 \bmod 192 = 140$

$5 \times 35 \bmod 192 = 175$

$6 \times 35 \bmod 192 = 18$

$7 \times 35 \bmod 192 = 52$

$8 \times 35 \bmod 192 = 88$

$9 \times 35 \bmod 192 = 123$

$10 \times 35 \bmod 192 = 158$

$11 \times 35 \bmod 192 = 1.$

Step 6: $PU = \{e, n\}$

$= \{35, 221\}$

Step 7: $PR = \{d, n\}$

$= \{11, 221\}$

Encryption:

$M = 92$

$C = M^e \bmod n$

$= 92^{35} \bmod 221$

$=$

Primitive root :

The primitive root of a prime number n is an integer r between [1, n-1] Such that the Values of r^x (mod n) where x is in the range [0, n-2] are different.

Ex:

2 is a primitive root mod 5, because for every number a relatively prime to 5, there is an integer z Such that $2^z \equiv a$.

All the numbers relatively prime to 5 are 1, 2, 3, 4 and each of these (mod 5) is itself (for Instance 2 (mod 5) = 2):

- $2^0 \equiv 1$,
  $1 \pmod 5 = 1$, So $2^0 \equiv 1$
- $2^1 \equiv 2$,
  $2 \pmod 5 = 2$, So $2^1 \equiv 2$
- $2^3 = 8$,
  $8 \pmod 5 = 3$, So $2^3 \equiv 3$
- $2^2 \equiv 4$,
  $4 \pmod 5 = 4$, So $2^2 = 4$

For every integer relatively prime to 5, there is a power of 2, that is Congruent.

Primitive Root of 11 is 7 :

(7^1) mod 11 = 7

(7^2) mod 11 = 5

(7^3) mod 11 = 2

(7^4) mod 11 = 3

(7^5) mod 11 = 10

(7^6) mod 11 = 4

(7^7) mod 11 = 6

(7^8) mod 11 = 9

(7^9) mod 11 = 8

(7^10) mod 11 = 1

(7^11) mod 11 = 7

$11\overline{)7} = 7$

$$\begin{array}{r} 1 \\ 11\overline{)14} \\ 11 \\ \hline 3 \\ \hline 1 \\ 11\overline{)21} \\ 11 \\ \hline 10 \\ \hline \end{array}$$

$$\begin{array}{r} 11\overline{)20} \\ 11 \\ \hline [illegible] \\ \hline \end{array}$$