R12032053

Unit. III

Methods of asymmetric key Cryptography
Asymmetric key Cryptography

Asymmetric Encryption:-

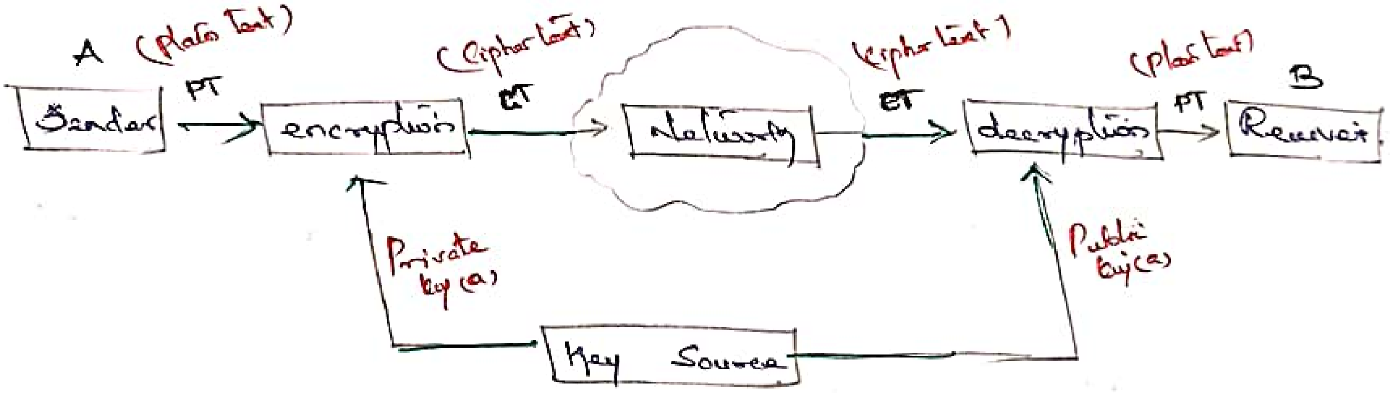
Principles of public key crypto systems:-

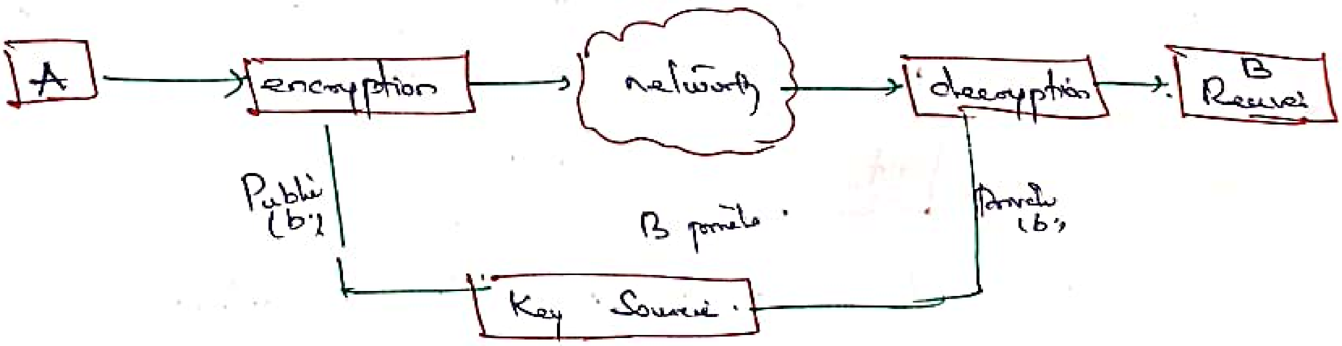
(Asymmetric key Cryptography)

There are two principles.

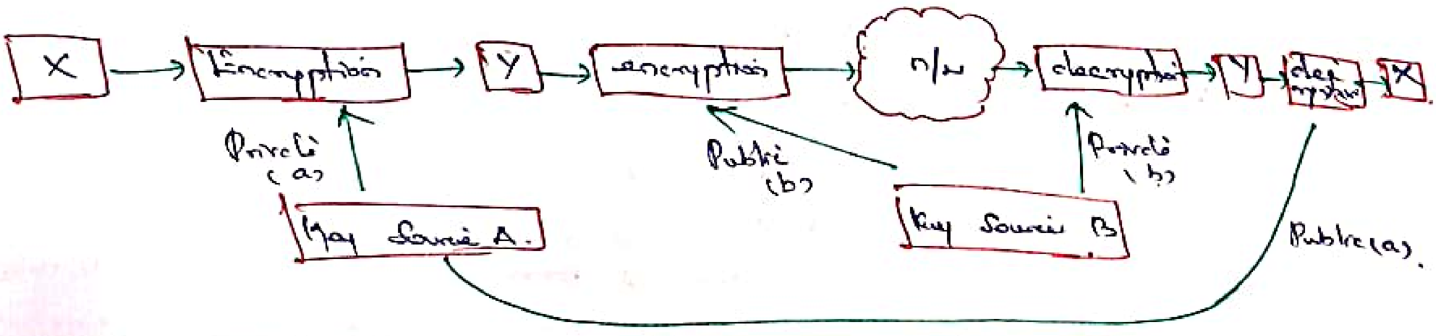
1. Authentication
2. Confidentiality

Authentication:-



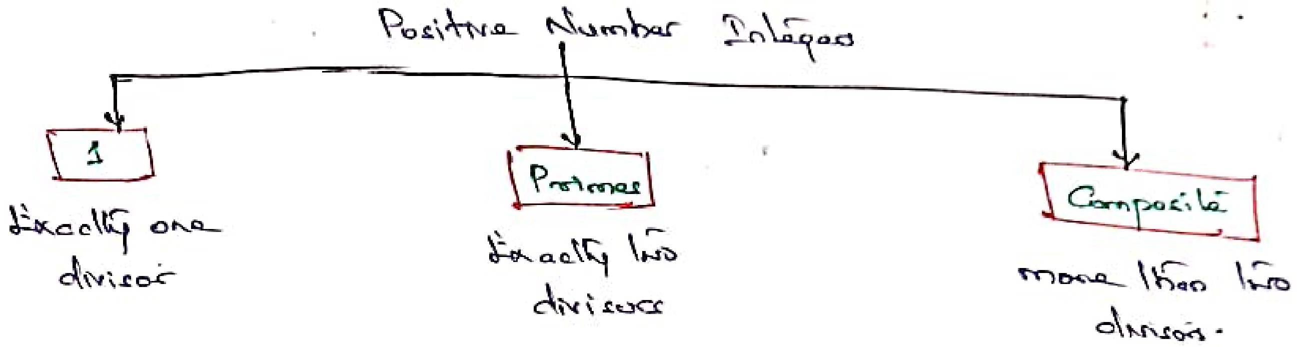


Confidentiality:-



Primes:-

- ★ Asymmetric key Cryptography Uses primes extensively



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

  i.e:- 1 or itself.

- ★ A Composite is a positive integer with 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 integer

  ⇒ 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.

[illegible] [illegible]

Associative [illegible] expression [illegible]

Euler's Theorem:

If a and n are relatively prime, then

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

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

≡ Congruent to [illegible]

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

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

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

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

$\boxed{6^{10} \bmod 11 = 1}$ ← It [illegible]

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

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

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

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

$\Rightarrow 12 \bmod 11$

$= 1$ Hence proved.

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

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

$\Rightarrow 3$

$$\begin{array}{r} 3 \\ 11\overline{)36} \\ \underline{33} \\ 3 \end{array}$$

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

$\Rightarrow 3^2 \bmod 11$

$\Rightarrow 9 \bmod 11$

$= 9$

$$\begin{array}{r} 2 \\ 11\overline{)27} \\ \underline{22} \\ 5 \end{array}$$

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

$\Rightarrow 27 \bmod 11$

$\Rightarrow 5$

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

$= 9^2 \bmod 11$

$= 81 \bmod 11$

$= 4$

$$\begin{array}{r} 7 \\ 11\overline{)81} \\ \underline{77} \\ 4 \end{array}$$

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

$= 3^5 \bmod 11$

$= 243 \bmod 11$

$$\begin{array}{r} 22 \\ 11\overline{)243} \\ \underline{22} \\ 23 \\ \underline{22} \\ 1 \end{array}$$

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

Practice:

$a = 8$ $n = 13$ $\gcd(8, 13) = 1$ ✓

$a = 5$ $n = 17$ ✓

$a = 4$ $n = 12$ ×

$a = 3$ $n = 23$ ✓

$a = 3$, $n = 17$

Eulers Totient Function :-
Euler

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

$n=3$ 1, 2 $\gcd(1,3) \to 1 \to$ RP
$\gcd(2,3) \to 2 \to$ R→P

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

(ii) If n is not prime

n is not prime

3 Cases

ⓐ $\phi(n) \to n = p \cdot q$ $\phi(p \cdot q) \Rightarrow \phi(p) \cdot \phi(q)$
$\Rightarrow (p-1)(q-1)$

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

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

$\gcd(1,6) \Rightarrow 1$ ✓ $= 1 \cdot 2 = \boxed{2}$
$\gcd(2,6) \Rightarrow 2$ ✗
$\gcd(3,6) \Rightarrow 3$ ✗
$\gcd(4,6) \Rightarrow 2$ ✗
$\gcd(5,6) \Rightarrow 1$ ✓

$6 \times \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{3}\right)$
$\overset{2}{\cancel{6}} \times \frac{1}{2} \times \frac{\cancel{2}}{\cancel{3}}$
$= 2$ //

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

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

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

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

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

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

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 = divide
[illegible] [illegible]

$a | p$ X

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

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

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

$\underline{p = 19}$ $\underline{a = 3}$

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

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

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

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

$= 8$

19) 27 (1
19
8

$3^{18} = (3^3)^6$

$= 8^6 \bmod 19$

$= (8^2)^3 \bmod 19$

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

19) 64 (3
57
7

$(8^2)^3 \bmod 19 = 7^3 \pmod{19}$

$= (7^2 \bmod 19) \cdot (7 \bmod 19)$

$= 11 \bmod 19 \cdot 7 \bmod 19$

$= (11 \times 7) \bmod 19$

$= 77 \pmod{19}$

19) 49 (2
38
11

19) 77 (4
76
1

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

Practice:-

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

Problems on FERMAT'S THEOREM :-

1. Using Formats Theorem, Find $\overset{a}{5}^{301} (\text{mod } \overset{p}{11})$

Sol:

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

$\gcd(a,p) = 1$

$\gcd(5,11) \Rightarrow 1 \qquad p = 11 \leftarrow$ if this condition true then apply Fermat's Theorem.

$a = 5 \qquad p = 11$

From Thm:

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

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

$\Rightarrow 5^{10} \text{ mod } 11 = 1$

Qn's

$4^{94} \text{ mod } 13 = ?$

$7^{501} \text{ mod } 13 = ?$

&

$2^{102} \text{ mod } 17 = ?$

$9^{2025} \text{ mod } 11 = ?$

Now:

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

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

$= 1^{30} \text{ mod } 11 \cdot 5^1 \text{ mod } 11$

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

$= 1.5 \text{ mod } 11$

$= 5$

$$\boxed{\therefore \; 5^{301} \text{ mod } 11 \Rightarrow 5}$$

2. Find $\overset{a}{3}^{201} \text{ mod } \overset{p}{7}$ Using Fermat's Theorem ?

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

$\gcd(a,p) = 1$

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

$a = 3 \qquad p = 7$

From Thm:

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

$\therefore 3^6 \text{ mod } 7 = 1$

$6 \overline{)201}$ 33
18
21
18
3

33×6
198
3
201

$7 \overline{)27}$ 3
21
1

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

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

$\Rightarrow 1 \cdot 6 \text{ mod } 7 = 6$//

$$\boxed{\therefore \; 3^{201} \text{ mod } 7 = 6}$$

DIFFIE - HELLMAN KEY EXCHANGE ALGORITHM:

- * It is not an encryption / decryption algorithm
- * It is used to exchange keys between Sender and Receiver.
- * It is an asymmetric key Cryptography.
- * Encryption involves both private and public key.

Now:

1. Let q be a prime number
2. Select α such that $\alpha < q$ and

α is primitive root of q

$5^1 \bmod 7 = 5$
$5^2 \bmod 7 = 4$
$5^3 \bmod 7 = 6$
$5^4 \bmod 7 = 2$
$5^5 \bmod 7 = 3$
$5^6 \bmod 7 = 1$
$\therefore$ 5 is a primitive root of 7.

To find Primitive root:

$$\alpha^1 \bmod q$$
$$\alpha^2 \bmod q$$
$$\alpha^3 \bmod q$$
$$\vdots$$
$$\alpha^{q-1} \bmod q$$

Should have the values

$\{1, 2, 3, \ldots\ldots q-1\}$

Check with all numbers less than 7 (ie: $q = 7$).

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

$3^1 \bmod 7 = 3$
$3^2 \bmod 7 = 2$
$3^3 \bmod 7 = 6$
$3^4 \bmod 7 = 4$
$3^5 \bmod 7 = 5$
$3^6 \bmod 7 = 1$
$\therefore$ 3 is a primitive root of 7.

So we can consider any integers of $\{1,2,3,4,5,6\}$ gives $\{5,4,6,2,3,1\}$ as all integers sequence of $\{1,2,3,4,5,6\}$ for $5^{q-1} \bmod 7$ and also $3^{q-1} \bmod 7$ etc can be consider as a primitive root.

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 (mod 5) = 1 , So $2^0 \equiv 1$ ← Primitive root

- $2^1 \equiv 2$,

  2 (mod 5) = 2 , So $2^1 \equiv 2$

- $2^3 \equiv 8$,

  8 (mod 5) = 3 , So $2^3 \equiv 3$

- $2^2 \equiv 4$,

  4 (mod 5) = 4 , So $2^2 \equiv 4$

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 mod 11 = 7.

(7^2) mod 11 = 5 = 49 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 | 7 = 7

1
11 | 14
11
3

1
11 | 21
11
10

Big Exponential Numbers:-

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

Default Values

$e = 6$ $m = 187$

$b = 11$ $c = 1$ (initial) (Constant)

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

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

$e' = 3$ $c = (b * c) \bmod m = (11 \times 121) \bmod 187 = 22$

$e' = 4$ $c = (b * c) \bmod m = (11 \times 22) \bmod 187 = 55$

$e' = 5$ $c = (b * c) \bmod m = (11 \times 55) \bmod 187 = 44$

$e' = 6$ $c = (b * c) \bmod m = (11 \times 44) \bmod 187 = \boxed{110}$ //.

Finally

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

This is the required result.

(or)

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

$= 121$

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

$= (121)^2 \bmod 187$

$= 14641 \bmod 187$

$= 55$

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

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

$= (121 \times 55) \bmod 187$

$= 6655 \bmod 187$

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

Y. Anbarasu. M.Sc., M.S., M.Tech., (PhD).,

DIFFIE HELLMAN KEY EXCHANGE ALGORITHM :

1. It is not an encryption/ Decryption algorithm
2. It is used to exchange keys between sender and receiver
3. It is a Asymmetric key cryptography
4. Encryption involve both private and public key

Algorithm:-

integer prime

Let q be a prime number

Given α, where $\alpha < q$ and

α is primitive root of q

~~Algorithm~~

Primitive root:

→ Assume a is a primitive root of p

→ If a mod p, a^2 mod p, a^3 mod p, ⋮ a^{p-1} mod p which results in 1, 2, 3, ... p-1 the values should not be repeated.

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

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 ?

≡ Congruent

On: q=13, α=7 ✓

On: q=11, α=7 ✓

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

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

≢ Not Congruent

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

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

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

User 'A' Key Generation:-

Assume $X_A = 3 < q = 7$

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

$\binom{X_A \;\; Y_A}{3, \;\; 6}$

$\boxed{Y_A = 6}$

$7 \overset{3}{\overline{)27}}$
$\underline{21}$
6

User 'B' Key Generation :-

Assume $X_B = 4$ & $q = 7$

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

$= 3^4 \bmod 7$

$$7\,\overline{)\,81}\quad 11,\ 7,\ 11,\ 7,\ 4$$

$\boxed{Y_B = 4}$ $\qquad \begin{matrix} X_B & Y_B \\ (4 & 4) \end{matrix}$

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 exchage is success.

Finally Calculate Secret Keys K_1 and K_2

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

$= 4^3 \bmod 7$

$$7\,\overline{)\,64}\quad 9,\ 63,\ 1$$

$= 64 \bmod 7$

$\boxed{K_1 = 1}$.

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

$$7\,\overline{)\,36}\quad 5,\ 35,\ 1$$

$= 6^4 \bmod 7$

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

$= 1^2$

$\boxed{K_2 = 1}$

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

$\boxed{K_1 = K_2}$

∴ The key exchange Successful:

THE CHINESE REMAINDER THEOREM:

The Chinese Remainder Theorem (CRT) is Used to Solve a Set of different Congruent equations with one Variable but different moduli, which are relatively prime, as shown below.

$$x_1 \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

CRT states that the above equations have a Unique Solution of the moduli are relatively prime.

Qn:

$$\underset{a_1}{x \equiv 1} \ (\bmod \underset{m_1}{5}) \ ; \ x \equiv \underset{a_2}{2} (\bmod \underset{m_2}{7}) \ ; \ x \equiv \underset{a_3}{3} (\bmod \underset{m_3}{9})$$

$$\boxed{x = \sum a_i \underset{?}{c_i} \ (\bmod \underset{?}{M})}$$

$$M = (m_1 \times m_2 \times m_3) \Rightarrow 5 \times 7 \times 9 \Rightarrow 315$$

$$\boxed{c_i = M_i \times (M_i^{-1} \bmod m_i)}$$

$$M_i = M/m_i \qquad \boxed{M = 315}$$

$$M_1 \Rightarrow \frac{M}{m_1} = \frac{315}{5} \Rightarrow 63$$

$$M_2 \Rightarrow \frac{M}{m_2} = \frac{315}{7} \Rightarrow 45$$

$$M_3 \Rightarrow \frac{M}{m_3} = \frac{315}{9} \Rightarrow 35$$

Now

$$\boxed{c_i = M_i \times (M_i^{-1} \bmod m_i)} \quad \text{formula}$$

$$c_1 = 63 \times (63^{-1} \bmod 5)$$

$$\Rightarrow 63 \times (\underbrace{3^{-1} \bmod 5}) \longrightarrow [3 \times x] \bmod 5 \Rightarrow 1$$

$$\Rightarrow 63 \times 2$$

$$\boxed{c_1 \Rightarrow 126}$$

$5 \overline{)63}$ = 12
5
13
10
3

$3^{-1} \bmod 5$

$3^{5-2} \bmod 5$

$3^{3} \bmod 5$

$= 2$

$5 \overline{)27}$ = 5
25
2

$C_2 \Rightarrow M_2 \times (M_2^{-1} \bmod m_2)$

$\Rightarrow 45 \times (45^{-1} \bmod 7)$

$\Rightarrow 45 \times (\underbrace{3^{-1} \bmod 7}) \longrightarrow (3 \times \underset{5}{\overset{\downarrow}{x}}) \bmod 7 \Rightarrow 1$

$\Rightarrow 45 \times 5$

$\boxed{C_2 \Rightarrow 225}$

$a^{P-2} = a^{7-2} = 5$

$45 \bmod 7$

$\underline{\underline{5}}$

a^{P-2}

$a^{7-2} = 5$

$45^{-1} \bmod 7$

$7 \,\overline{)\,45\,}$ quotient 6; $45 - 42 = 3 \Rightarrow 3^{-1} \bmod 7$

$3^{7-2} \bmod 7$

$3^5 \bmod 7$

$7 \,\overline{)\,243\,}$ quotient 34; $243 - 21 = 33$; $33 - 28 = \boxed{5}$ ✓

$C_3 \Rightarrow M_3 \times (M_3^{-1} \bmod m_3)$

$\Rightarrow 35 \times (35^{-1} \bmod 9)$

$\Rightarrow 35 \times (\underbrace{8^{-1} \bmod 9}) \longrightarrow (8 \times \underset{\uparrow}{x}) \bmod 9$

$\Rightarrow 35 \times 8$

$\boxed{C_3 \Rightarrow 280}$

$35^{-1} \bmod 9$

$9 \,\overline{)\,35\,}$ quotient 3; $35 - 27 = 8$

$8^{-1} \bmod 9.$

$8^1 \bmod 9 = 8$

$8^2 \bmod 9 = 1$

$8^2 \cdot 8^2 \cdot 8^2 \cdot 8^1 \bmod 9$

$1 \cdot 1 \cdot 1 \cdot 8 = 8$ //

Substitute in formula:-

$\boxed{X \Rightarrow \Sigma\, a_i C_i \bmod M}$

$\Rightarrow [a_1 C_1 + a_2 C_2 + a_3 C_3] \bmod M$

$\Rightarrow [1 \times 126 + 2 \times 225 + 3 \times 280] \bmod 315$

$\Rightarrow [126 + 450 + 840] \bmod 315$

$X \Rightarrow (1416) \bmod 315$

$\boxed{X \Rightarrow 156}$

$315 \,\overline{)\,1416\,}$ quotient 4; $1416 - 1260 = 156$

Home Work:

(1)
$X \equiv 2 \pmod 3$
$X \equiv 3 \pmod 5$
$X \equiv 2 \pmod 7$

(2)
$X \equiv 4 \pmod 3$
$X \equiv 4 \pmod 5$
$X \equiv 6 \pmod 7$

(3)
$X \equiv 3 \pmod 5$
$X \equiv 1 \pmod 7$
$X \equiv 6 \pmod 8$

$156 \equiv 1 \pmod 5$; $156 \equiv 2 \pmod 7$; $156 \equiv 3 \pmod 9$

$5 \,\overline{)\,156\,}$ quotient 31; $156 - 15 = 6$; $6 - 5 = 1$

$7 \,\overline{)\,156\,}$ quotient 22; $156 - 14 = 16$; $16 - 14 = 2$

$9 \,\overline{)\,156\,}$ quotient 17; $156 - 9 = 66$; $66 - 63 = 3$

v.v.I.

RSA Algorithm :-

ALGORITHM:

Rivest Shamir Adleman

< Public
Private

1979

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 : $M < n$

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

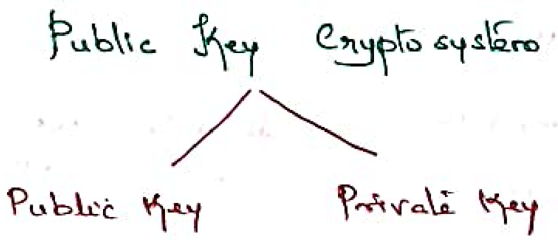
2time [illegible]
$C = P^e \bmod n$
$P = c^d \bmod n$

DECRYPTION by USER B WITH USER B's PRIVATE KEY

Cipher text : C

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

Extended Euclidean algorithm



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 values 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: Euler 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:-

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

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

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

$481 \bmod 120 = 1$

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

d ↓

$13 \times 7 = 91 \bmod 120$ ✗

$13 \times 17 = 221 \bmod 120$ ✗

$13 \times 27 = 351 \bmod 120$ ✗

$13 \times 37 = 481$ ✓

$120 \overline{)481}$ 4; 480; 1

Extended Euclidean algorithm also used to find d value.

Now to perform Encryption and Decryption:

Encryption:-

$C = M^e \bmod n$

$= 5^{13} \bmod 155$

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

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

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

$= 5^4 \bmod 155$

$= 625 \bmod 155$

$\boxed{C = 5}$

$5^2 = 25 \bmod 155$ ✗

$5^3 = 125 \bmod 155$ ✗

$5^4 = 625 \bmod 155$ ✓

$155 \overline{)625}$ 4; 620; 5

ie: $5^4 \bmod 155$

$= 625 \bmod 155$

$= 5$

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

Decryption :-

$$M = c^d \bmod n$$
$$= 5^{37} \bmod 155$$
$$= (5^{13})^2 \cdot (5^4)^2 \cdot 5^3 \bmod 155$$
$$= (5)^2 \cdot (5)^2 \cdot 5^3 \bmod 155$$
$$= 5^4 \cdot 5^3 \bmod 155$$
$$= 5 \cdot 5^3 \bmod 155$$
$$= 5^4 \bmod 155$$
$$\boxed{M = 5}$$

i.e. $5^{37} \bmod 155 = 5$

We know.

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

$(5^{13})^2 = 5^{26}$
$(5^4)^2 = 5^8$
$5^3 = 5^3$
$\Rightarrow 5^{26} \cdot 5^8 \cdot 5^3$
$= 5^{26+8+3}$
$\boxed{= 5^{37}}$

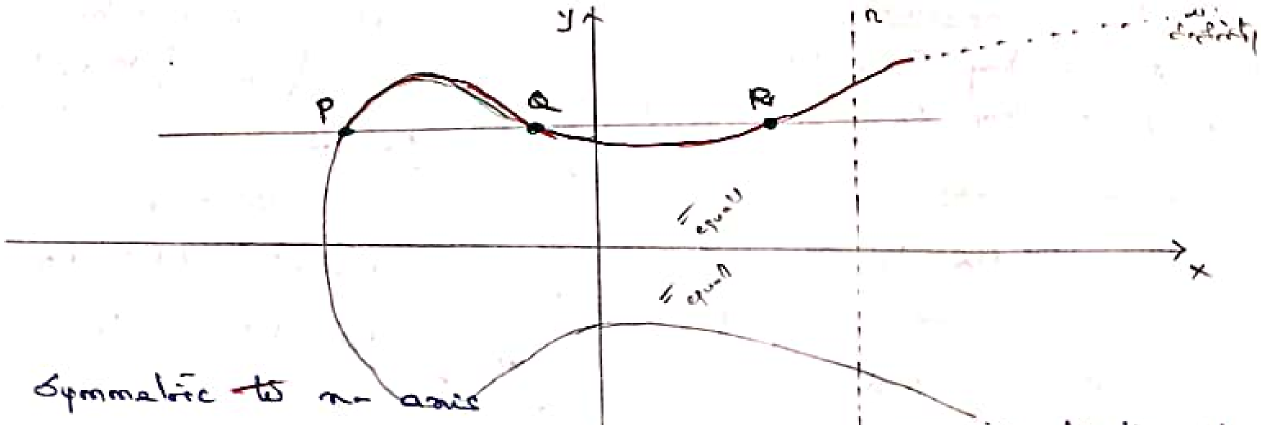
Elliptic Curve Cryptography: (ECC)

- It is asymetric public key cryptography. Similar to RSA.
- It provides equal security with smaller key size (as compared to RSA) as compared to non-ECC algorithms

i.e. Small key size and high security

- It makes use of Elliptic Curves. public key Cryptography
- Elliptic Curves are defined by some mathematical functions - Cubic functions
- Where public key → Encryption and private key - Decryption

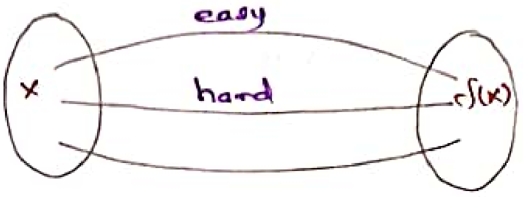
Eg: $\boxed{y^2 = x^3 + ax + b}$ // equation of degree 3..



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

A Trapdoor function is a fn that is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information called the trapdoor.

$A \longrightarrow B$ is easy
$\longleftarrow$ Inverse not easy



easy is given "t" → trapdoor values

Let $E_p(a,b)$ be the elliptic curve.

Consider the equation $\boxed{Q = KP}$

where Q, P → points on curve and $K < n$

If K and P → given, it should be easy to find Q, but if we know Q and P, it should be extremely difficult to find K. (This is called discrete logarithmic problem).

ECC - Algorithm:-

ECC - Key Exchange:

Global Public Elements:

1) $E_q(a,b)$: elliptic curve with parameters a, b and $\boxed{q}$.

↑ Prime no: or form 2^m

2) G : point on the elliptic curve.

User A Key Generation:-

Select private key n_A, $n_A < n$

Calculate public key P_A, $P_A = n_A \times G$

User B Key Generation:-

Select private key n_B, $n_B < n$

Calculate public key P_B, $P_B = n_B \times G$

Calculation of Secret key by User A:-

$$K = n_A \times P_B$$

Calculate of Secret key by User B:-

$$K = n_B \times P_A$$

Encryption:-

Cipher point will be

$$\boxed{C_m = \{ KG, P_m + KP_B \}}$$

Decryption:-

$$KG \times n_B$$

$$P_m + KP_B - (KG \times n_B)$$

$$\therefore P_m + KP_B - KP_B$$

$$\boxed{= P_m.}$$

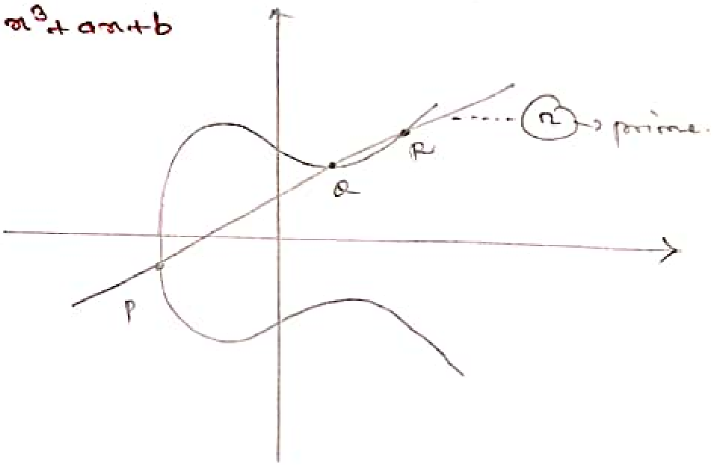
So receiver gets the same point.

Elliptic Curve Cryptography:-

Advantage:-

- * It Uses shorter key size
- * It provides higher Security
- * It Consumes low Computational power
  - ie: suitable for Smartphones and tablets.

$y^2 = x^3 + ax + b$



→ Symmetric - x axis

→ 3 points at max Can be generated

→ $Q = kP$ ← random integer $< n$

easy

$P^{-1}Q = k$

Problem on RSA:-

Qn: $P = 17$, $q = 11$, $m = 88$ from the given e : not 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:

$$\gcd(e, 160) = 1, \qquad 1 < e < \phi(n).$$
$$1 < \underset{\overset{\uparrow}{e}}{\boxed{7}} < 160$$

$$d \equiv e^{-1} \bmod \phi(n)$$
$$d = 7^{-1} \bmod 160$$
$$7 \times \underset{\overset{\uparrow}{23}}{d} \bmod 160 = 1$$

$$\begin{array}{r l} & \;1 \\ 160 & \overline{)161} \\ & \;160 \\ \hline & \;\;\;1 \end{array}$$

$$7 \times 23 \bmod 160 = 1$$
$$161 \bmod 160 = 1$$
$$\boxed{\therefore\ d = 23}$$

How 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:-

$M = c^d \bmod n$

$= 11^{23} \bmod 187$

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

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

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

$\boxed{M = 88}$

11 273 570
11 273 482
88

$11^1 = 11 \bmod 187$

$= 11$

$11^2 = 121 \bmod 187$

$= 121$

$11^4 = 14641 \bmod 187$

$= 55$

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

$= 55^2 \bmod 187$

$= 3025 \bmod 187$

$= 33$

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

$= 33^2 \bmod 187$

$=$

$= 154$

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
   $\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
5. Calculate d
   $d = e^{-1} (\bmod\ \phi(n))$
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

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

$(n \times 7) \bmod 160$

$= 23$ $\qquad (23 \times 7) \bmod 160$

ie $n = 23$ $\qquad 161 \bmod 160$

$\equiv 1$

$PU = \{7, 187\}$

$PR = \{23, 187\}$

Encryption and Decryption:-

Encryption:-

Plain → 2 digit decimal	
plaintext	$M < n$ 187
Ciphertext	$C = M^e \bmod n$

$Pu \to \langle 7, 187 \rangle$

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

$M = 88$

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

Decryption:-

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

Now,

$$\begin{aligned}M &= C^d \bmod n\\ &= 11^{23} \bmod 187\\ &= 88\end{aligned}$$

(Equal)

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

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

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

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

$\boxed{d = 11}$

$0\times 35 \bmod 192 = 0$
$1\times 35 \bmod 192 = 35$
$2\times 35 \bmod 192 = 70$
$3\times 35 \bmod 192 = 105$
$4\times 35 \bmod 192 = 140$
$5\times 35 \bmod 192 = 175$
$6\times 35 \bmod 192 = 18$
$7\times 35 \bmod 192 = 53$
$8\times 35 \bmod 192 = 88$
$9\times 35 \bmod 192 = 123$
$10\times 35 \bmod 192 = 158$
$11\times 35 \bmod 192 = 1$

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

$= \{35, 221\}$

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

$= \{11, 221\}$

Encryption:

$M = 92$

$C = M^e \bmod n$

$= 92^{35} \bmod 221$

$= (92^{32}) \cdot 92^2 \cdot 92^1 \bmod 221$

$= 1\times 66\times 92 \bmod 221$

$= 6072 \bmod 221$

$\boxed{C = 105}$

$92^1 \bmod 221 = 92$
$92^2 \bmod 221 = 8464 \bmod 221$
$= 66$
$(92)^4 \bmod 221 = (66)^2 \bmod 221$
$= 4356 \bmod 221$
$= 157$
$(92)^8 \bmod 221 = (92^4)^2 \bmod 221$
$= (157)^2 \bmod 221$
$= 24649 \bmod 221$
$= 118$
$(92)^{16} \bmod 221 = (92^8)^2 \bmod 221$
$= (118)^2 \bmod 221$
$= 13924 \bmod 221$
$= 1$
$(92)^{32} \bmod 221 = (92^{16})^2 \bmod 221$
$= 1^2 \bmod 221$
$= 1$

Decryption:-

$M = C^d \bmod n$

$= 105^{11} \bmod 221$

$= 105^8 \cdot 105^2 \cdot 105^1 \bmod 221$

$= 118\times 196\times 105 \bmod 221$

$= 2428440 \bmod 221$

$\boxed{M = 92}$

$105^8 = (105^4)^2 \bmod 221$
$= 183^2 \bmod 221$
$= 33489 \bmod 221$
$= 118$

$105 \bmod 221 = 105$
$105^2 \bmod 221 = 11025 \bmod 221$
$= 196$
$(105)^4 \bmod 221 = (105^2)^2 \bmod 221$
$= 196^2 \bmod 221$
$= 38416 \bmod 221$
$= 183$

Qn: Perform encryption and decryption using RSA algorithm.

$p=3$; $q=7$, $e=5$; $M=10$
$p=5$; $q=13$; $e=5$; $M=8$
$p=7$; $q=17$, $e=11$; $M=11$
$p=7$; $q=13$, $e=11$; $M=2$
$p=17$; $q=23$, $e=9$; $M=7$