USN | | | | | | | | | | |

Internal Assessment Test II- Dec. 2022

Sub:	Cryptography					Sub Code:	18CS744	Branch:	CSE
Date:	02/12/2022	Duration:	90 mins	Max Marks:	50	Sem/Sec:	C		OBE

	Answer any FIVE FULL questions	MARKS	CO	RBT
1 a).	What is Diffie Helman key exchange? How does it work?	[06]	CO2	L2
b).	Suppose that two parties A and B wish to set up a common secret key between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Determine the common secret key that they can use for sharing the confidential message.	[04]	CO2	L3
2.	What is an Abelian Group? Check whether the $\langle Z_7 - \{0\}, * \rangle$ forms the Abelian group? Verify with all the required group properties to be satisfied to be an abelian group.	[10]	CO3	L3

3 a).	What is Elliptic curve? How would you add points P and Q on an elliptic curve $E_p(a,b)$ *when*, *i*). $P = Q$ *ii*). $P \neq Q$	[06]	CO3	L2
3 b).	Check whether the point (6, 6) will be a point on the Elliptic curve $E_{11}(1,1)$	[04]	CO3	L3
4	Consider the Elliptic curve $E_{11}(1, 6)$. The cryptosystem parameters are $E_{11}(1, 6)$ and $G = (2, 7)$. B's private key is $n_B = 7$. **a.** Find B's public key P_B. **b.** A wishes to encrypt the message $Pm = (10, 9)$ and chooses the random value $k = 3$. Determine the ciphertext Cm. **c.** Show the calculation by which B recovers Pm from Cm.	[10]	CO3	L3
5	Where does the IP traffic is verified before it enters the organizational LAN? Explain the inbound and outbound process of IP traffic processing.	[10]	CO3	L3
6	Define IP Security. How confidentiality and Authentication based security is enabled through transport and tunnel modes. Explain the procedure.	[10]	CO3	L2

Solutions:

1. What is Diffie Helman key exchange? How does it work?

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel (over Internet).This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Working of Algorithm:

Consider two parties, 'A' and 'B' that need to agree upon a single shared key for the duration of their current session. Both 'A' and 'B' will be knowing about a common modulus 'p' and the generator 'g' of the selected modulus.

In order to exchange the shared secret, both will participate in the following sequence of steps.

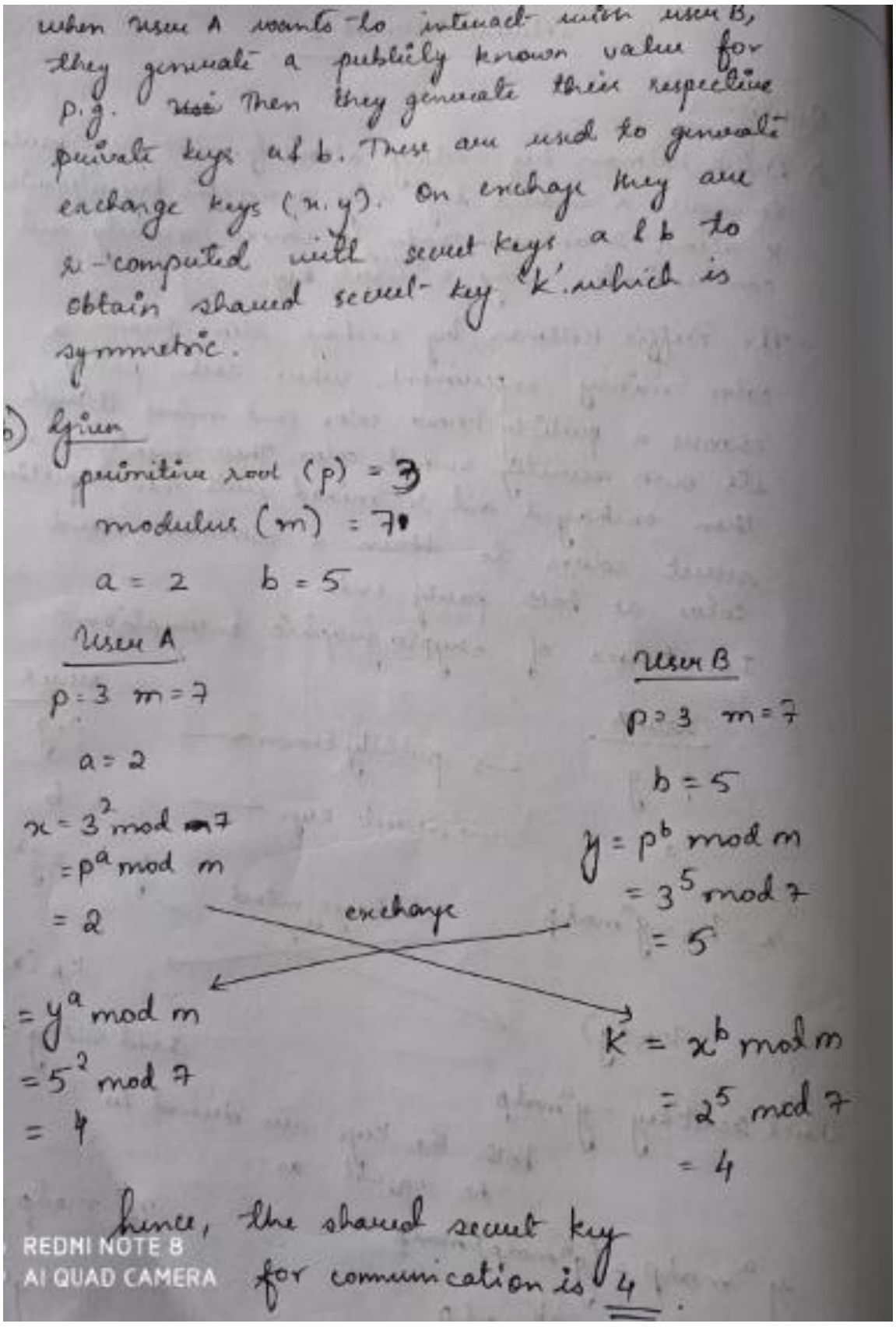
User A	User B
Selects Public Keys: **p, g**	Selects Public Keys: **p, g**
Private key selected is: **a**	Private key selected is: **b**
Public key generated: $x = g^a mod\ p$	Public key generated: $y = g^b mod\ p$
Exchange generated public keys	
Key received: y	Key received: x
Generates shared secret: $k_A = y^a mod\ p$	Generates shared secret: $k_B = x^b mod\ p$
Algebraically it can be shown that these 2 keys are equal and the same	
$(g^b mod\ p)^a mod\ p$	$(g^a mod\ p)^b mod\ p$
Above equation can also be written as $(g^a mod\ p)^b mod\ p$	$(g^a mod\ p)^b mod\ p$
Both the derived keys are found to be equal. Ie, $k_A = k_b$	
Now both the users 'A' and 'B' can use the shared secret key for encrypting the messages during the current session.	

1b. Suppose that two parties A and B wish to set up a common secret key between them using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Determine the common secret key that they can use for sharing the confidential message.

XA=2

XB=5, g=3

KA= KB=4



Q2.

What is an Abelian Group? Check whether the $\langle Z_7 - \{0\}, * \rangle$ forms the Abelian group? Verify with all the required group properties to be satisfied to be an abelian group.

Question-2

Abelian group is a group that also follows commutative property.

A group is a set of values which uses a binary operator $(*, +)$ exhibits the properties of closure, associativity, identity and inverse.

Given : $\langle Z_7 - \{0\}, * \rangle$

$\{1, 2, 3, 4, 5, 6, 7\}$

$-3\ -2\ -1\ 1\ 2\ 3\ 4$

$a * e = e * a = a$

$a * a^{-1} = e = a^{-1} * a$

(i) Closure property
The set of integers are closed on multiplication operation on Z_7 w/o $\{0\}$.

(ii) Associativity
$a(bc) = (ab)c$ stands true for all computations done on the given set

(iii) Identity
The identity element exists '1'
$a * e = e * a = a \Rightarrow e = 1$

(iv) Inverse
The inverse of each element exists which stands true $a * a^{-1} = e = a^{-1} * a$

(v) Commutative
The operations $a * b = b * a$ stands true on the given set and thus exhibits the property.

Hence, $\langle Z_7 - \{0\}, * \rangle$ is an abelian group as it satisfies all properties.

Abelian group is a group that also follows commutative property.

A group is a set of values which uses a binary operator $(*, +)$ exhibits the properties of closure, associativity, identity and inverse.

Given : $\langle Z_7 - \{0\}, * \rangle$

$\{1, 2, 1, 4, 5, 6, 7$

$-3\ -2\ -1\ \ 1\ 2\ 3\ 4$

$a * e = e * a = a$

$a * a^{-1} = e = a^{-1} * a$

(i) Closure property
The set of integers are closed on multiplication operation on Z_7 w/o $\{0\}$.

(ii) Associativity
$a*(b*c) = (a*b)*c$ stands true for all computations done on the given set

(iii) Identity
The identity element exists '1'
$a * e = e * a = a \Rightarrow e = 1$

(iv) Inverse
The inverse of each element exists which stands true $a * a^{-1} = e = a^{-1} * a$

(v) Commutative
The operations $a * b = b * a$ stands true on the given set and thus exhibits the property.

Hence, $\langle Z_7 - \{0\}, * \rangle$ is an abelian group as it satisfies all properties.

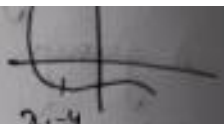
3.

(a) An ellip

the given equation:-

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

where a & b are constants



$4a^3 + 27b^2 \neq 0$

To add 2 points P & Q on the curve: when $E_p(a,b)$

(i) P = Q

assuming $P = Q = (x, y)$

we find $\lambda = \frac{3x^2 + a}{2y} \bmod p$

then, $x_3 = \lambda^2 - x - x \bmod p$

$y_3 = \lambda(x - x_3) - y \bmod p$

where p is the elliptic curve limit.

& $(x_3, y_3) = (x, y) + (x, y)$.

(ii) P ≠ Q

assuming $P = (x_1, y_1)$ $Q = (x_2, y_2)$

we find $\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod p$

then $x_3 = \lambda^2 - x_1 - x_2 \bmod p$

$y_3 = \lambda($

(b) given point

curve $E_{11}(1,1)$

$x = 6$, $y = 6$, p , a , b

$p = 11$, $a = 1$, $b = 1$

hence, if the point lies on the elliptic curve it should satisfy :-

$$y^2 \bmod p = x^3 \bmod p + ax + b \bmod p$$

$$6^2 \bmod 11 = 6^3 + 1(6) + 1 \bmod 11$$

$$36 \bmod 11 = 223 \bmod 11$$

$$3 = 3 \quad //$$

hence, the point (6,6) lies on elliptic curve $E_{11}(1,1)$.

Question-4

Given :- $E_{11}(1,6)$

$p = 11$ $a = 1$ $b = 6$

$G = (2,7)$

B's private key $= n_B = 7$

a. Find B's public key P_B

$$P_B = n_B G = 7 * (2,7)$$

$$= (2,7) + (2,7) + (2,7) + (2,7) + (2,7) + (2,7) + (2,7)$$

$x_1 y_1$ $x_2 y_2$ $x_3 y_3$ $x_4 y_4$

$x, y \rightarrow (2,7) + (2,7)$

$$\lambda = \frac{3x^2 + a}{2y} \bmod p$$

$$= \frac{3(2)^2 + 1}{2 \times 7} \bmod 11$$

$$= \frac{13}{14} \bmod 11$$

multiplicative inverse :- $14 * x \bmod 11 = 1$

$14 * \underline{4} \bmod 11 = 1$

$= 13 * 14^{-1} \bmod 11$

$= 13 * 4 \bmod 11$

$\lambda = 8 //$

$x_1 = \lambda^2 - x - x \bmod 11 = 64 - 2 - 2 \bmod 11$

$= 60 \bmod 11$

$= 5 //$

$y_2 = \lambda(x - x_1) - y \bmod 11 = 8(2 - 5) - 7 \bmod 11$

$= -31 \bmod 11$

$= 2 //$

$(x_1, y_1) = (5, 2)$

$(x_2, y_2) = (x_1, y_1) + (2, 7)$

$= (5, 2) + (2, 7)$

P: x_1, y Q: x_2, y_2

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod 11 = \frac{7 - 2}{2 - 5} \bmod 11$$

$$= \frac{5}{-3} \bmod 11$$

multiplicative inverse

$= -5 \times 4 \bmod 11$

$x_2 = \lambda^2 - x_1 - x_2$

$= 4 - 5 - 2 \mod 11$

$= -3 \mod 11 = 8$

$y_2 = \lambda(x_1 - x_2) - y_1 \mod 11$

$= 2(5-8) - 2 \mod 11$

$= 3$

$(x_2, y_2) = (8, 3)$

$(x_3, y_3) = (x_2, y_2) + (2, 7)$

$= (8, 3) + (2, 7)$

$x_1 \uparrow y_1 \quad x_2 \uparrow y_2$

$P \quad Q$

$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \mod p = \frac{7-3}{2-8} \mod 11$

$= \frac{4}{-6} \mod 11 \quad -\frac{2}{3}$

$= -2 \times 4 \mod 11$

$= 3$

$x_3 = \lambda^2 - x_1 - x_2 \mod 11$

$= 9 - 8 - 2 \mod 11$

$= 10$

$y_3 = \lambda(x_1 - x_3) - y_1 \mod 11$

$= 3(8 - 10) - 3 \mod 11$

$= 2$

$x_3, y_3 = (10, 2)$

$x_4, y_4 = (x_3, y_3) + (2, 7)$

$= (10, 2) + (2, 7)$

$x_1 \uparrow y_1 \quad x_2 \uparrow y_2$

$P \quad Q$

$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \mod p = \frac{7-2}{2-10} \mod p \; 11 = \frac{5}{-8} \mod 11$

$= -5 * 7 \mod 11$

$= -35 \mod 11 = 9.$

$= \frac{2}{5} \bmod 11$ → inverse

$= 2 * 9 \bmod 11$

$= 18 \bmod 11$

$\lambda = 7$ //

$x_6 = \lambda^2 - x_1 - x_2 \bmod 11$

$= 49 - 7 - 2 \bmod 11$

$= 7.0$ //

$y_6 = \lambda(x_1 - x_6) - y_1 \bmod 11$

$= 7(7-7) - 9 \bmod 11$

$= -9 \bmod 11 = 2$ //

$x_6, y_6 = (7,2)$

public key of B = (7,2) //

(b) $P_m = (10,9)$ $k = 3$

$C_m = [kG, P_m + kP_B]$

$= [3(2,7), (10,9) + [3(7,2)]]$

C_1 C_2

C_1 → from previous calculations

$C_1 = (2,7) + (2,7) + (2,7) = (x_2, y_2) = (8,3)$

$C_2 \longrightarrow 3(7,2)$

$= (7,2) + (7,2) + (7,2)$

$x_1\ y_1$ $x_2\ y_2$

$x_4 = \lambda^2 - x_1 - x_2 \mod 11$

$= (9)^2 - 10 - 2 \mod 11 = 3$

$y_4 = \lambda(x_1 - x_4) - y_1 \mod 11$

$= 9(10-3) - 2 \mod 11$

$= 6$

$x_4, y_4 = (3, 6)$

$x_5, y_5 = (x_4, y_4) + (2, 7)$

$= (3, 6) + (2, 7)$

x_4 ↑ y_1 (P) $\quad x_2$ ↑ y_2 (Q)

$\lambda = \frac{7-6}{2-3} \mod 11 = \frac{1}{-1} \mod 11$

$= -1 \mod 11 = 10$

$x_5 = \lambda^2 - x_1 - x_2 \mod 11$

$= 100 - 3 - 2 \mod 11 = 7$

$y_5 = \lambda(x_1 - x_5) - y_1 \mod 11$

$= 10(3-7) - 6 \mod 11$

$= 9$

$(x_5, y_5) = (7, 9)$

$(x_6, y_6) = (x_5, y_5) + (2, 7)$

$= (7, 9) + (2, 7)$

x_1 ↑ y_1 (P) $\quad x_2$ ↑ y_2 (Q)

$\lambda = \frac{y_2 - y_1}{} \mod 11 = 7 - 9$

$(8,3) + (8,3)$

$$\lambda = \frac{3x^2 + a}{2y} \bmod 11$$

$$= \frac{193}{6} * 2 \bmod 11$$

(6 → inv)

$$= 1 //$$

$$x_1 = 1 - 8 - 8 \bmod 11 = 7$$

$$y_1 = 1(8-7) - 3 \bmod 11 = 9$$

$x_2\ y_2 = (7,9) + (8,3)$

$x_1\ y_1 \quad x_2\ y_2$

$$\lambda = \frac{-6}{\quad} \bmod 11 = 5 //$$

$$x_2 = 25 - 7 - 8 \bmod 11 = 10$$

$$y_2 = 5(7-10) - 9 \bmod 11 = 9$$

$x_2, y_2 = (10,9)$

$x_3, y_3 = (10,9) + (8,3)$

$$\lambda = \frac{3-9}{8-10} \bmod 11 = \frac{-6}{-2} = 3$$

$$x_3 = 9 - 10 - 8 \bmod 11 = 2$$

$$y_3 = 3(10-3) - 9 \bmod 11 = 1$$

$x_3\ y_3 = 2, 1$

now, $C_2 = (10,9) + (x_2, y_2)$

$= (10,9) + (3,5)$

$x_1 \; y_1 \quad x_2 \; y_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod 11 = \frac{5-9}{3-10} \bmod 11$$

$$= \frac{-4}{-7} \bmod 11$$

$= 4 * 8 \bmod 11$

$= 10 //$

$x_3 = \lambda^2 - x_1 - x_2 \bmod 11$

$= 100 - 10 - 3 \bmod 11$

$x_3 = 10 //$

$y_3 = \lambda(x_1 - x_3) - y_1 \bmod 11$

$= 10(10-10) - 9 \bmod 11 = 2 //$

$C_2 = (10,2)$

hence, ciphertext

$C_m = [(8,3), (10,2)]$

(c) B recovers P_m from C_m with decryption.

$P_m = C_2 - n C_1$

$= (8,3) - 7(8,3)$

$7(8,3) = (8,3) + (8,3) + (8,3) + (8,3) + (8,3) + (8,3) + (8,3)$

x_1, y_1 x_2, y_2 x_3, y_3 x_4, y_4 x_5, y_5 x_6, y_6

for x_1, y_1 ...

$$\lambda = \frac{3x^2 + a}{2y} \bmod 11$$

$$= \frac{3(7)^2 + 1}{2(2)} \bmod 11$$

$$= \frac{148}{4} \bmod 11 = 37 \bmod 11$$

$$= 4 //$$

$$x_1 = \lambda^2 - x - x \bmod 11$$

$$= 16 - 7 - 7 \bmod 11$$

$$= 2 //$$

$$y_1 = \lambda(x - x_1) - y \bmod 11$$

$$= 4(7 - 2) - 2 \bmod 11$$

$$= 7 //$$

$$(x_1, y_1) = (2, 7)$$

$$(x_2, y_2) = (x_1, y_1) + (7, 2)$$

$$= \underset{P}{(2, 7)} + \underset{Q}{(7, 2)}$$

x_1 ↑ y_1 (P) $\quad$ x_2 ↑ y_2 (Q)

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod 11 = \frac{2 - 7}{7 - 2} \bmod 11$$

$$= \frac{-5}{5} \bmod 11$$

$$= 10 //$$

$$x_2 = \lambda^2 - x_1 - x_2 \bmod 11$$

$$= 100 - 2 - 7 \bmod 11 = 3$$

$P_m = (8,3) - (x_6, y_6)$

$= (8,3) - (3,8)$

$= (8,3) + (3,-8)$

$\lambda = \frac{-8-3}{3-8} \bmod 11 = \frac{-11}{-5} \bmod 11$

$= 11 * 9 \bmod 11$

$= 0$

$P_m x = -8-3 \bmod 11 = 10$ //

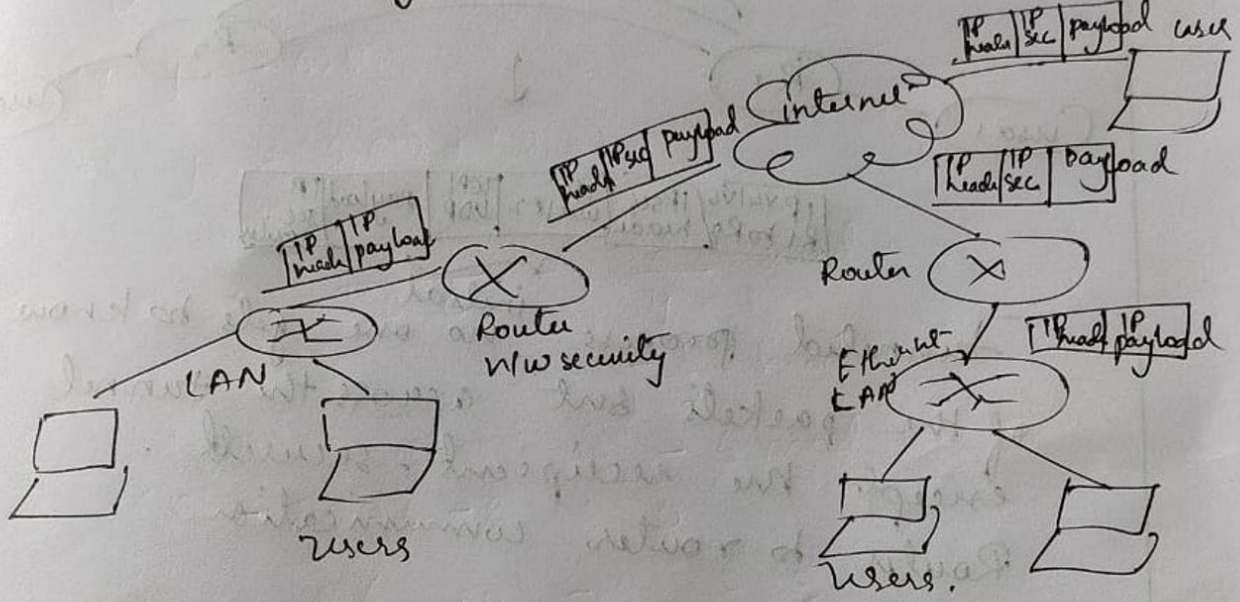
$P_m y = -3 \bmod 11 = 9$ //

hence, message is recovered successfully

Question-6

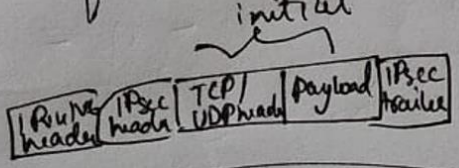
IP security refers to the security exhibited at the network layer when messages are passed through networking devices.

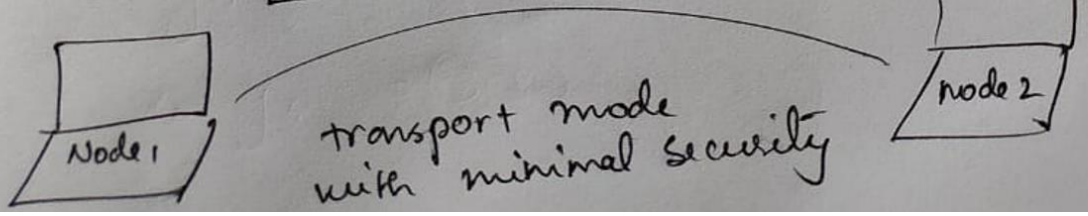
IP security is added through confidentiality & authentication using various protocols, ESP, AH etc.



The main modes enabled through transport and tunnel transfers.

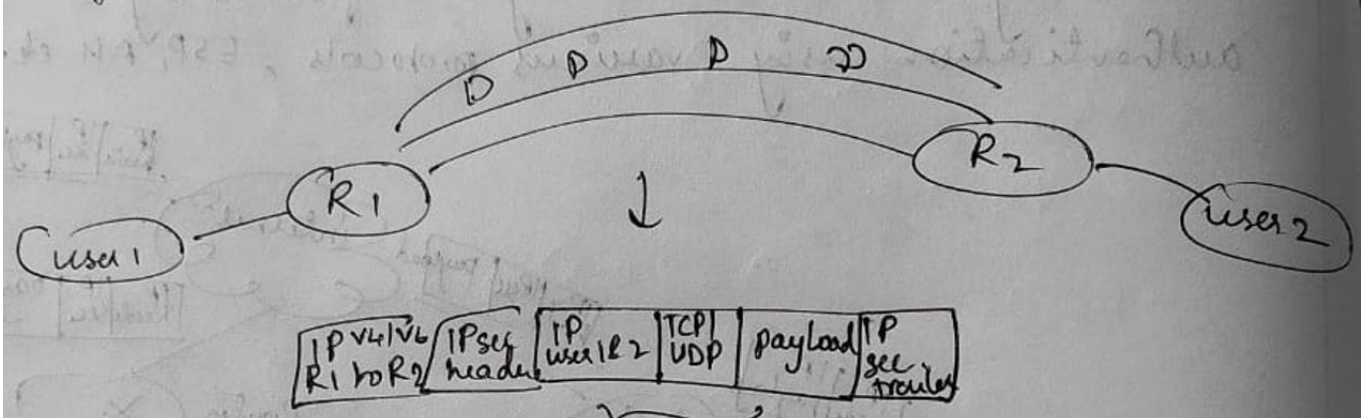
In transport transfer, the package gets packed with IP security header & trailer first and then the external IP v4 | v6 headers. It is used for node to node communications.





transport mode with minimal security

In tunnel mode transfer the data packets are already encrypted with IP headers of nodes before adding IP sec and then again re-encapsulating with IP headers for router to router transmissions.



initial

tunneled process no one gets to know of the packets sent across the tunnel except the recipient. secured.

Router to router communication

a. $P_B = n_B \square G = 7 \square (2, 7) = (7, 2)$. This answer is seen in the preceding table.
b. $C_m = \{kG, P_m + kP_B\}$
$= \{3(2, 7), (10, 9) + 3(7, 2)\} = \{(8,3), (10, 9) + (3, 5)\} = \{(8, 3), (10, 2)\}$
c. $P_m = (10, 2) – 7(8, 3) = (10, 2) – (3, 5) = (10, 2) + (3, 6) = (10, 9)$