

School of Computer Science and Engineering

Winter Semester 2023-2024

Continuous Assessment Test – II

SLOT: E2+TE2

Programme Name & Branch: B.Tech-CSE

Course Name & code: BCSE309L & Cryptography and Network Security

Class Number (s): Applicable to All

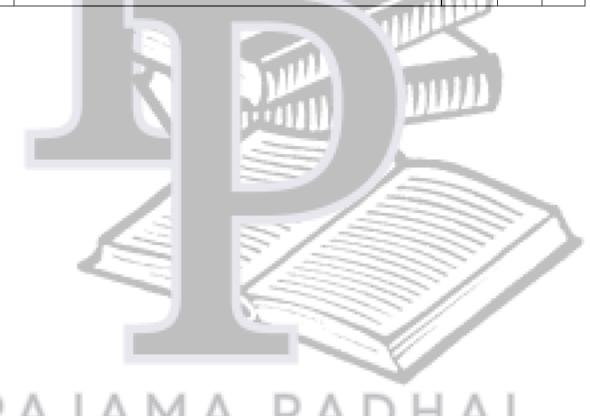
Faculty Name (s): Applicable to All

Exam Duration: 90 Min. Maximum Marks: 50

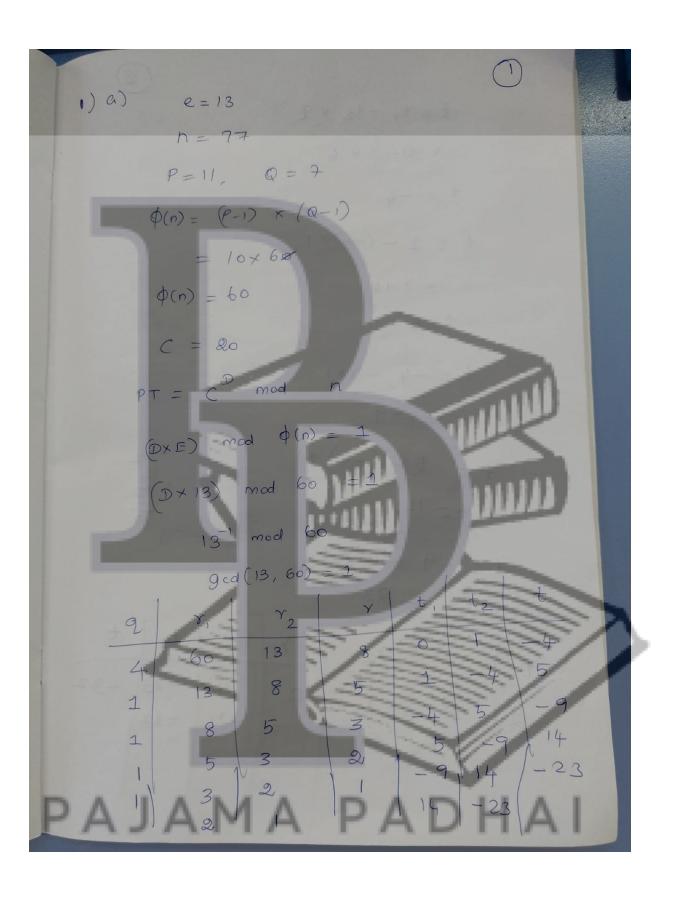
Answer ALL the questions

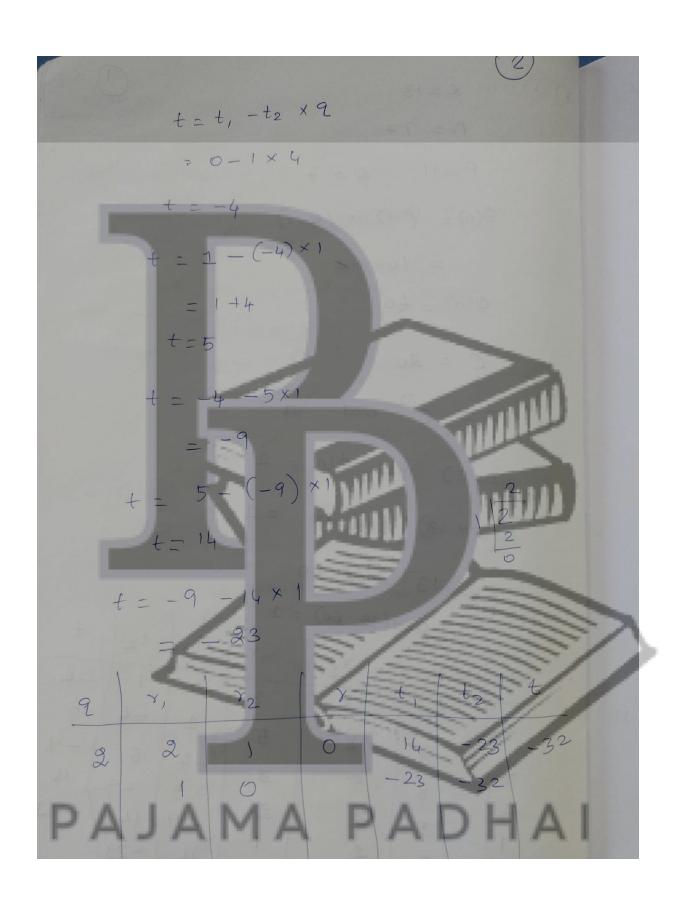
		100		
Q.No.	Question	Max	CO	BL
		Marks		
1.	a) You have captured the ciphertext C=20 sent to a user whose	5	CO2	BL3
	public key is e=13, n=77, in an RSA Public Key System. Is it			
	possible to compute the plain text M?			
	b) Describe the man-in-the-middle attack and show that the	5		\sim
	shared secret key between the communicators remains the			\rightarrow
	same for the inputs p=11, g=2, $X_A = 9$, and $X_B = 4$.	5/		
2.	Suppose Alice and Bob use an Elgamal scheme with a common	10	CO2	BL5
	prime $q = 157$ and a primitive root $\alpha = 5$.			
	i. If Bob has public key $Y_B = 10$ and Alice chose the random			
	integer $k = 3$, what is the ciphertext of $M = 9$?			
D	ii. If Alice now chooses a different value of k so that the			
	encoding of $M = 9$ is $C = (25, C2)$, what is the integer $C2$?			
3.	Perform Elliptic Curve Encryption using $E_{13}(10,6)$ and	10	CO2	BL3
	$G(5,5)$. The value of the private key, $n_b = 5$, $P_m = (6, 8)$, and			
	chooses the random k value as 2.			
			l	

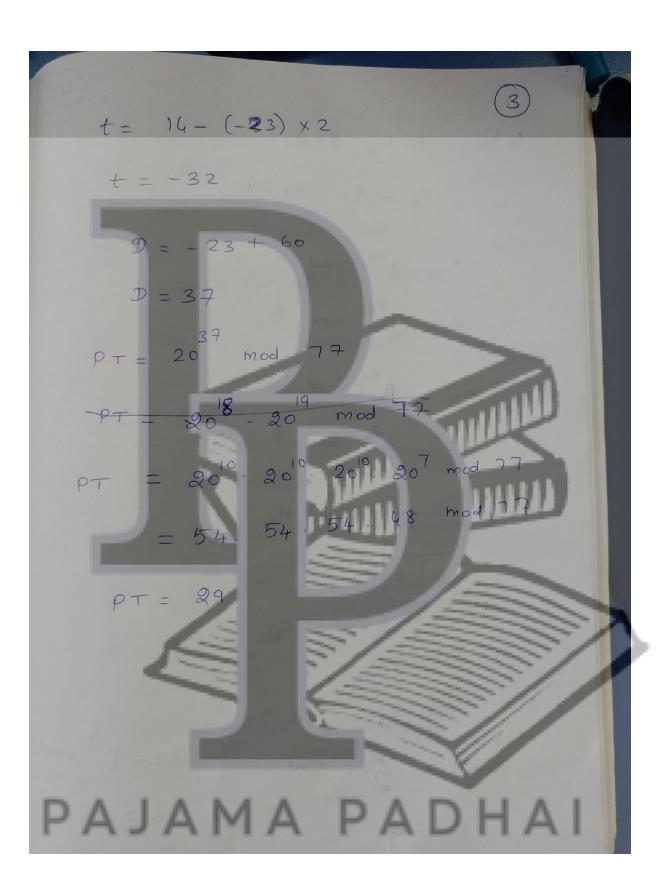
4.	a) Compute the value of the padding field, length filed, and number of blocks in MD5 if the length of the message 4000 bits.	5	CO3	BL4
	b) Find the output of the the logical functions F, G, H, and I used in MD5 round opeartions if the initial value of the buffers are as follows:	5		
	A – 01234567			
	B – 89abcdef			
	C – fedcba98			
	D - 76543210			
5.	Using the ElGamal Digital signature scheme, User A chose p=13,		CO3	BL4
<i>J</i> .	q=2, private key $X_A = 3$, $H(m) = 11$, $k = 5$. He announces the		CO3	DLT
	global components publicity.			
	(i) Find the publich key Y _A	2		
	(ii) How user A does the signing process to compute (S1, S2)? (iii) How user B does the verification process?	4 4		
	(iii) flow user b does the verification process:	milit		

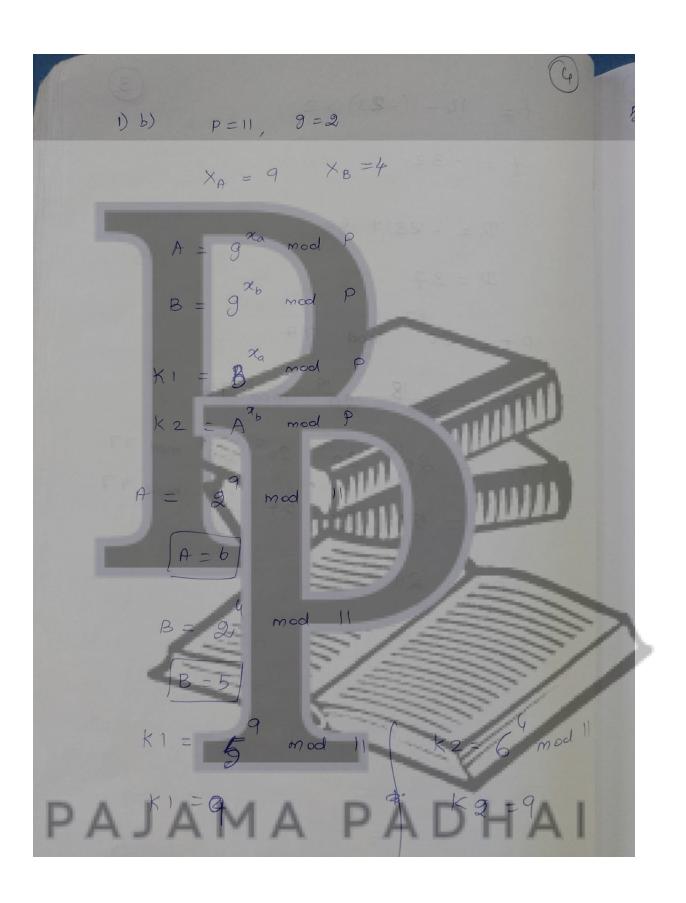


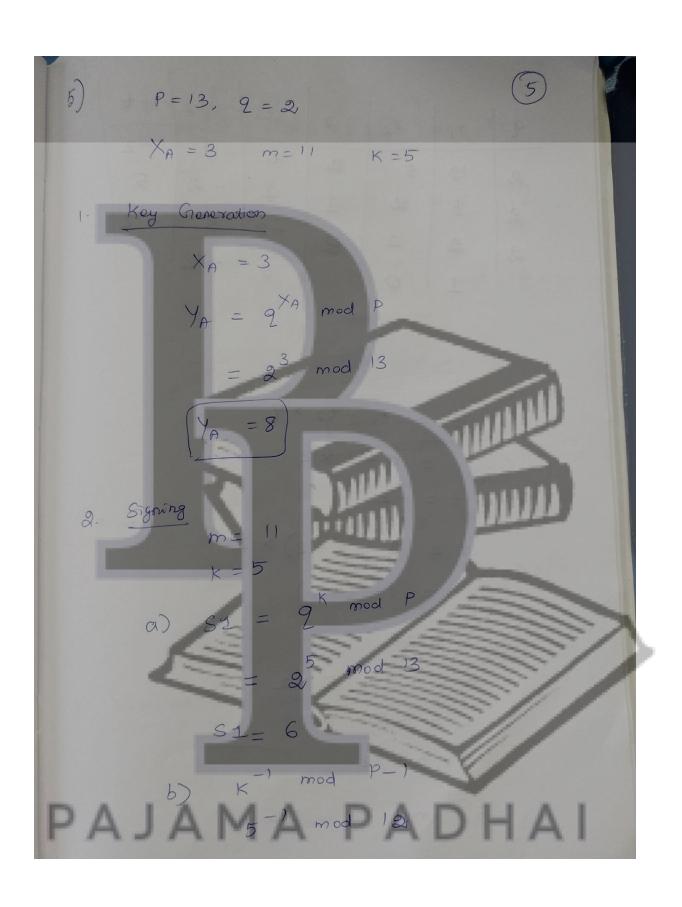
PAJAMA PADHAI

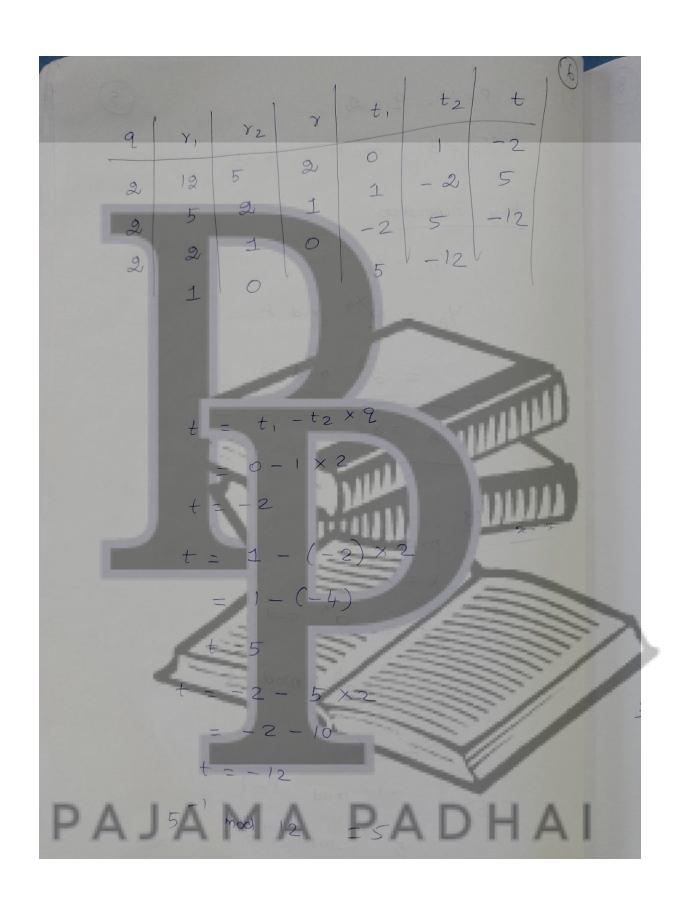


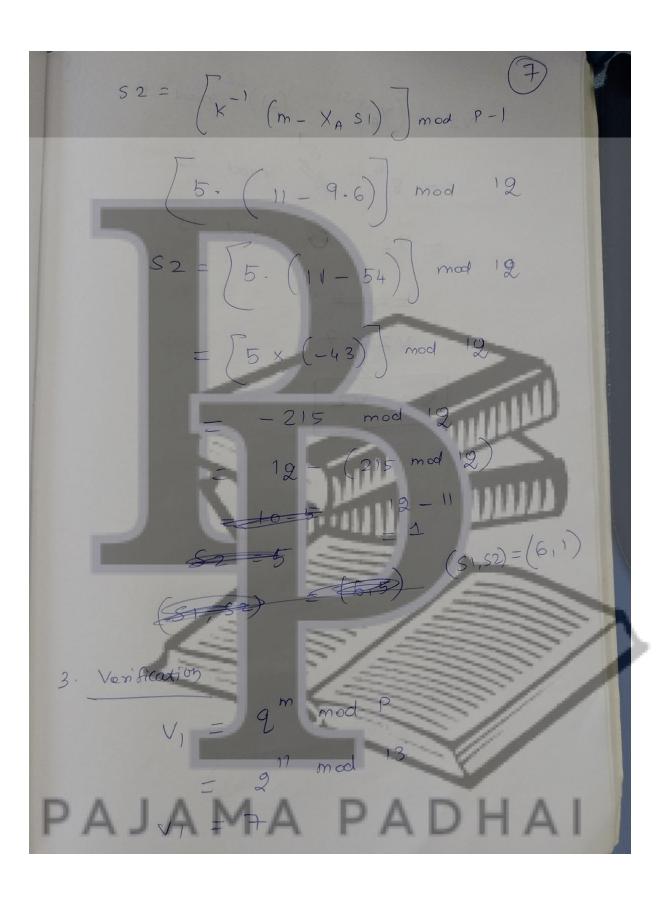


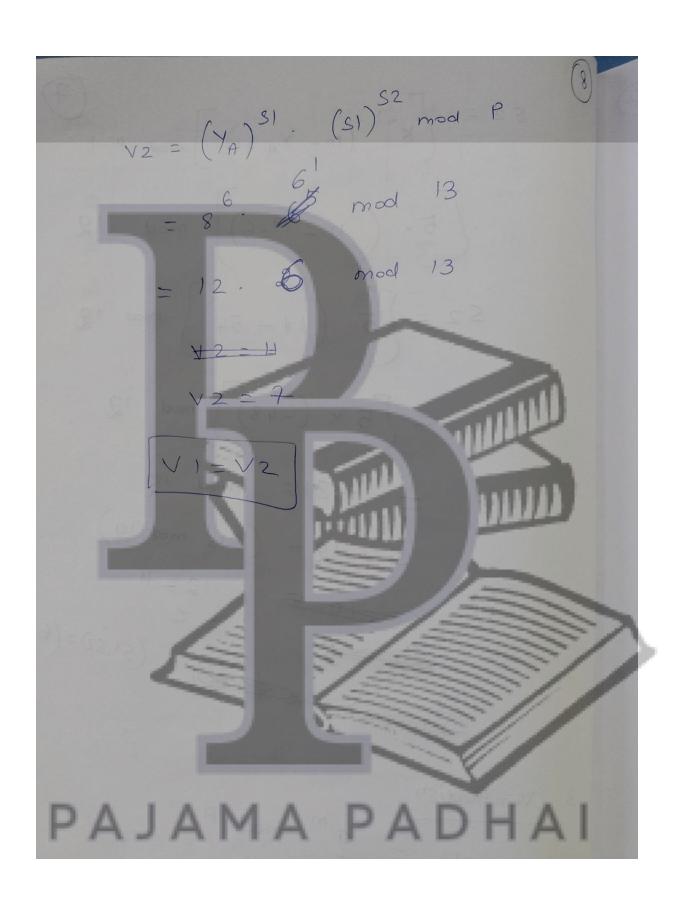


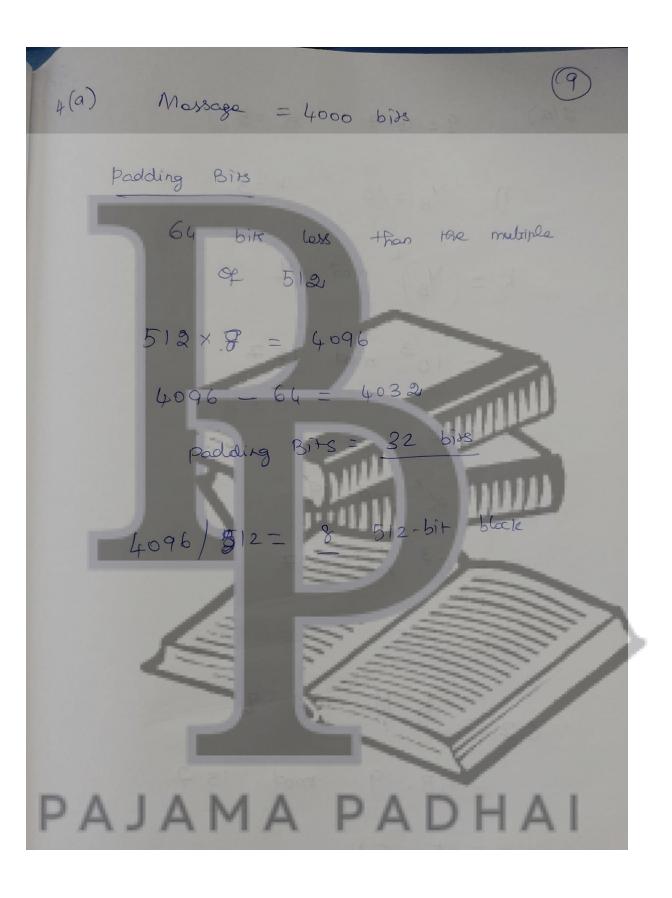


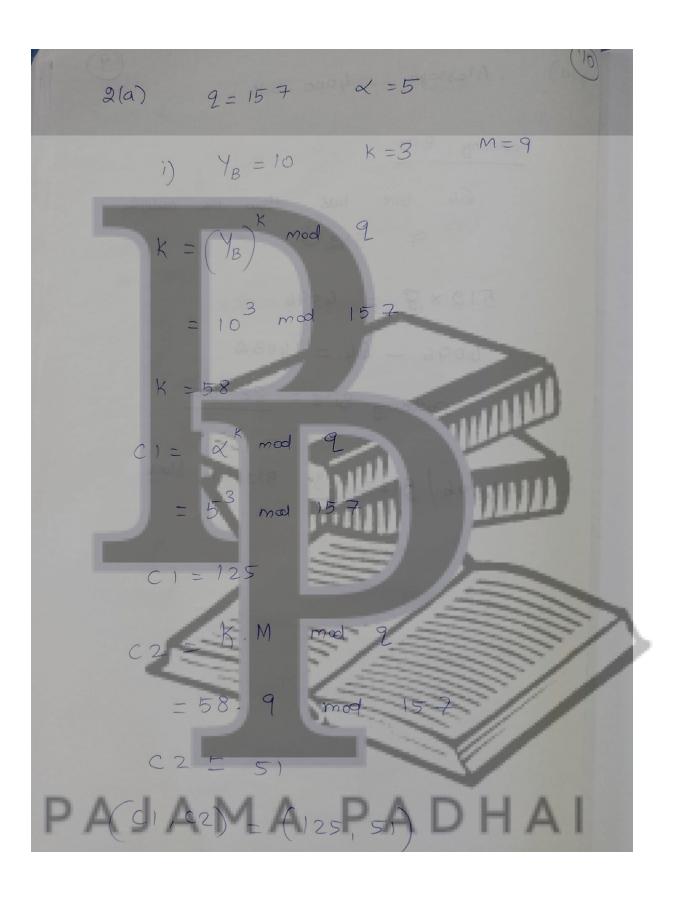


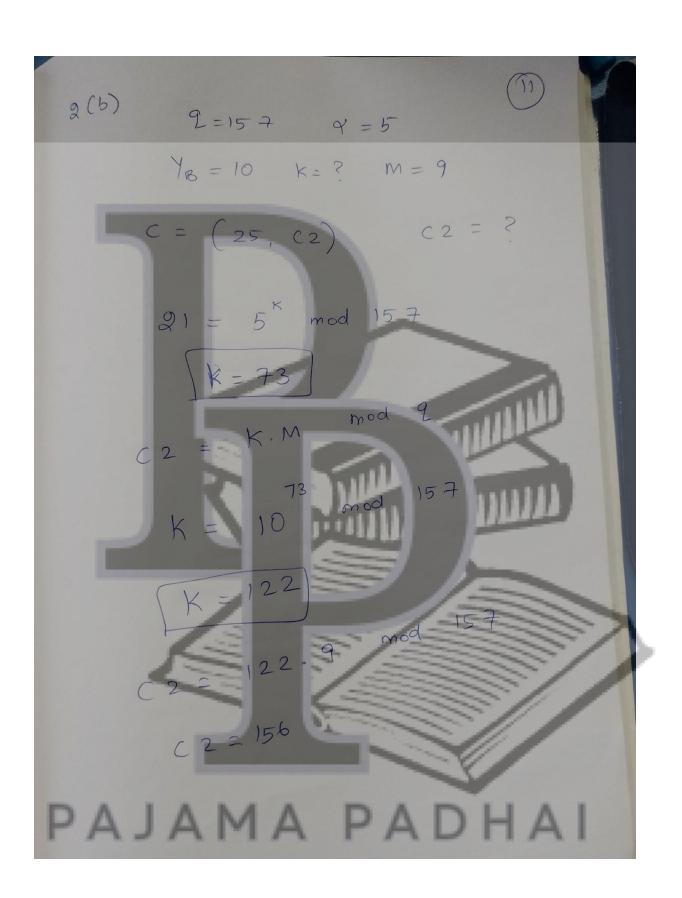












3. ECC Solution

Perform Elliptic Curve Encryption and Decryption using $E_{13}(10,6)$ and G(5,5). And the value of the private key, $n_b=5$ & chooses the random k value as 2.

Find the corresponding public key (P_b) of the given private key

$$P_h = n_h * G = 5 * (5,5)$$

And as we know the curve is $E_{13}(10,6)$,

$$p = 13$$
, $a = 10$, $b = 6$

So, first let us calculate

$$2*G = G + G$$

Where G = (5,5).

$$2 * G = 2 * (5,5) = (7,4)$$

After we find 2 * G, we perform the next step, which is to find $3 * G = (X_3, Y_3)$

$$(X_3, Y_3) = 3 * G = 2 * G + G = (7,4) + (5,5)$$

Here we have,

$$X_1 = 7$$
 , $Y_1 = 4$

$$X_2 = 5$$
 , $Y_2 = 5$

we find λ

$$\lambda = \frac{Y_2 - Y_1}{X_2 - X_1} \mod p = \frac{5 - 4}{5 - 7} \mod 13$$
$$= \frac{1}{(-2)} \mod 13 = \frac{-1}{2} \mod 13 = -1 * 2^{-1} \mod 13$$

,

$$2^{-1} \mod 13 = 7$$

$$\lambda = -1 * 2^{-1} \mod 13 = -7 \mod 13$$

$$= 13 - 7 \mod 13 = 6$$

And now we got $\lambda = 6$, we find X_3 and Y_3 ,

Finding X_3 ,

$$X_3 = (\lambda^2 - X_1 - X_2) \mod p = (6^2 - 7 - 5) \mod 13$$

= $(36 - 7 - 5) \mod 13 = 24 \mod 13 = 11$

Finding Y_3 ,

$$Y_3 = (\lambda * (X_1 - X_3) - Y_1) \mod p = (6 * (7 - 11) - 4) \mod 13$$

= (-28) mod 13 = 13 - 28 mod 13 = 13 - 2 = 11

Hence, we have

$$3 * G = (X_3, Y_3) = (11, 11)$$

And now that we have 3 * G and 2 * G, we can now evaluate 5 * G,

$$5 * G = 3 * G + 2 * G = (11,11) + (7,4)$$
 (20)

Here let us consider

$$(X_3, Y_3) = 5 * G$$

 $(X_1, Y_1) = (11,11)$
 $(X_2, Y_2) = (7,4)$

First, we have to find λ ,

$$\lambda = \frac{Y_2 - Y_1}{X_2 - X_1} \mod p = \frac{4 - 11}{7 - 11} \mod 13$$
$$= \frac{7}{4} \mod 13 = 7 * 4^{-1} \mod 13$$

So first we can find $4^{-1} \mod 13$,

Let us start from Z = 1,

e i i		B. ALLES
	Z	$\frac{Z*4-1}{13}$ is integer?
	1	No
	2	No
	3	No
	4	No
	5	No
	6	No
	7	No
	8	No
	9	No
	10	Yes
		and the same of th

$$4^{-1} \mod 13 = 10$$

$$\lambda = 7 * 4^{-1} \mod 13 = 7 * 10 \mod 13 = 70 \mod 13 = 5$$

And now we got $\lambda = 5$, we find X_3 and Y_3 ,

Finding X_3 ,

$$X_3 = (\lambda^2 - X_1 - X_2) \mod p = (5^2 - 11 - 7) \mod 13$$
$$= (25 - 11 - 7) \mod 13 = 7 \mod 13 = 7$$

Finding Y_3 ,

$$Y_3 = (\lambda * (X_1 - X_3) - Y_1) \mod p = (5 * (11 - 7) - 11) \mod 13$$

= 98 mod 13 = 9

Hence, we have

$$(X_3, Y_3) = (7, 9)$$

$$5 * G = 3 * G + 2 * G = (11,11) + (7,4) = (7,9)$$

Hence,

$$P_b = 5 * G = 5 * (5,5) = (7,9)$$

 $P_b = (7,9)$

Let us now perform encryption on plain text $P_m(6,8)$ and random number k=2. Obtain the cipher text C_m .

$$C_m = \{k * G, P_m + k * P_b\}$$

First let us consider the first part of C_m , ,

$$k * G = 2 * G = 2 * (5,5) = (7,4)$$

 $k * G = (7,4)$

Now let us move to the second part, where we have to find $P_m + k * P_b$,

First, we have to find $k * P_b$,

$$k * P_b = 2 * (7,9)$$

And let,

$$(X_3, Y_3) = 2 * P_b = P_b + P_b$$

$$X = 7, Y = 9$$

And we find λ , by substituting the X, Y

$$\lambda = \frac{(3*X^2+a)}{2*Y} \mod p = \frac{(3*7^2+10)}{2*9} \mod 13$$
$$= \frac{157}{18} \mod 13 = 157*18^{-1} \mod 13$$

Let us start from Z = 1,

Z	$\frac{Z*18-1}{13}$ is integer?
1	No
2	No
3	No
4	No
5	No
6	No
7	No
8	Yes

the value of $18^{-1} \mod 13 = 8$

So, substituting $18^{-1} \bmod 13$,

$$\lambda = 157 * 18^{-1} \mod 13 = 157 * 8 \mod 13$$

= 1 * 8 \mod 13 = 8

So, we got,

$$\lambda = 8$$
 , $X = 5$ and $Y = 5$

Now, we find X_3 and Y_3 ,

Finding X_3 ,

$$X_3 = (\lambda^2 - 2 * X) \mod p = (8^2 - 2 * 7) \mod 13$$

= $(64 - 14) \mod 13 = 50 \mod 13 = 11$

Finding Y_3 ,

$$Y_3 = (\lambda * (X - X_3) - Y) \mod p = (8 * (7 - 11) - 9) \mod 13$$

= $(8 * (-4) - 9) \mod 13 = (-32 - 9) \mod 13$
= $(-41) \mod 13 = 13 - 41 \mod 13 = 13 - 2 = 11$

Hence, we have

$$(X_3, Y_3) = (11, 11)$$

So,

$$k * P_b = 2 * (7,9) = (X_3, Y_3) = (11,11)$$

So, now that we have found $k \ast P_b$, we can compute the 2nd part of \mathcal{C}_m , Let,

$$(X_3, Y_3) = P_m + k * P_b,$$

We know that,

$$P_m = (6.8)$$

$$P_m + k * P_b = (X_3, Y_3) = (6.8) + (11.11)$$

Let us consider,

$$(X_1, Y_1) = (6,8)$$

$$(X_2, Y_2) = (11,11)$$

First, we have to find λ ,

$$\lambda = \frac{Y_2 - Y_1}{X_2 - X_1} \mod p = \frac{11 - 8}{11 - 6} \mod 13$$
$$= \frac{3}{4} \mod 13 = 3 * 5^{-1} \mod 13$$

So first we can find $5^{-1} \mod 13$,

Let us start from Z = 1,

Z	$\frac{Z*5-1}{13}$ is integer?
1	No
2	No
3	No
4	No
5	No
6	No
7	No
8	Yes
	The second second

$$5^{-1} \mod 13 = 8$$

$$\lambda = 3 * 5^{-1} \mod 13 = 3 * 8 \mod 13$$

$$= 24 \mod 13 = 11$$

And now we got $\lambda = 11$, we find X_3 and Y_3 ,

Finding X_3 ,

$$X_3 = (\lambda^2 - X_1 - X_2) \mod p = (11^2 - 11 - 6) \mod 13$$
$$= (121 - 11 - 6) \mod 13 = 104 \mod 13 = 0$$

Finding Y_3 ,

$$Y_3 = (\lambda * (X_1 - X_3) - Y_1) \mod p = (11 * (6 - 0) - 8) \mod 13$$

$$= 58 \mod 13 = 6$$

Hence, we have

$$(X_3, Y_3) = (0,6)$$

$$P_m + k * P_b = (6.8) + (11.11) = (0.6)$$

Now that we have also got the second component of the \mathcal{C}_m , we have completed calculating the cipher text, ,

$$C_m = \{k * G, P_m + k * P_b\} = \{(7,4), (0,6)\}$$

MD5 Solution

word A: 01 23 45 67 word B: 89 AB CD EF word C: FE DC BA 98 word D: 76 54 32 10

Round	Primitive function g	g(b, c, d)
1	F(b, c, d)	(b ∧ c) ∨ (b ∧ d)
2	G(b, c, d)	$(b \wedge d) \vee (c \wedge d)$
3	H(b, c, d)	b⊕c⊕d
4	I(b, c, d)	c ⊕ (b ∨ d)

PAJAMA PADHAI

```
1000 1001 1010 1011 1100 1101 111, 1111
                                                            AND
                     1111 1110 1101 1100 1011 1010 1001
                                                      1000
                     1000 1000 1000 1000 1000 1000 1000
                                                      1000
   BN C =
                010 010 0101 0100 0011 0010 0001
                                                         0000
       JB =
                                                         0000
                                                   000
                              0101 0100 0011
                                             0010
                        0110
                0111
                                                         2000
                                             0016
                                                   000/
                                       001)
                             0101 0100
                        0110
                 0 114
  7 BAD =
                                                         1000
                                                  (000
                              1000 (ON 1000
                                             (000)
                       1000
                (000)
  -BAC =
                      1110 11011100 1011 1010 1001
                                                         1000
                11111
                                  C B
                                                         8
                              1
                 F
       So, first F = FEDC BA98
      Protos 9
       Be 1000 1001 1010 1011 1100 1101
                                                        AND
                            0 00 0011 0010
       D2 01117 0110
                       0101
                                                  000
           0000 0000 0000
BND =
                                                   1000 JAND
                                      1010
                                             001
                           1100 -1011
                    1/01
         1111
                1110
      C:
                                            1110
                           1011 1100
                                      1101
                     1010
    7D' = 1000
                1001
                                                  1000
                           000 1000
                                            1000
                     1000
                                      1000
                1000
          1000
C170 -
```

PAJAMA PADHAI

```
0000 1000 1000 (OR)
               1000 1000
                             1000 1000
       CATO=
                        1000
               0000 0000
       BND=
                                       1000 1000 1000
              1000
                             1000
                                  1000
                   1000
                        1000
            9= 8
                             8
B 1000 1001 1010
                                             1110
                                        1101
                           101
                                  1100
                                                 1000
                                             1001
                                        1010
                           1100
                                  1011
        C: 1111 1116 1101
                                        011) 0111 0111
                                                  0000 0X01
                           0111
  BAC DIII
                                 0111
                11101110
                                       0010 0001
                                 0011
                           0100
         1010 0110 1110
                                                 0-11
                                             0110
                                       0101
                                 0100
         0000 0001 0010
                           0011
                                                 7
                                             6
                                         5
                                 4
                            3
               0/234567
                                                1110 1111
                                           1101
                                1011 1100
                          1610
                    1001
                                                1110
         B= 1000
                                           1101
                                1011 1100
                          1010
                   1001
      1000 ECT
                                1011 1100 1101
                          1010
                                                     1000
                                          1070 (001
                    1001
            1000
                               1100 1011
BVID
                        1101
                   011/011/01/01/1011/01/01/01/01/01/
                FEDC BA98
                         8888
                      4567
              0123
       H 16 2
              7777 7777
```

PAJAMA PADHAI