VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

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

Q.No.	Question	Max Marks	CO	BL
1.	a) You have captured the ciphertext C=20 sent to a user whose public key is e=13, n=77, in an RSA Public Key System. Is it possible to compute the plain text M?	5	CO2	BL3
	b) Describe the man-in-the-middle attack and show that the shared secret key between the communicators remains the 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 prime q = 157 and a primitive root α = 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 ? 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?	10	CO2	BL5
3.	Perform Elliptic Curve Encryption using $E_{13}(10,6)$ and $G(5,5)$. The value of the private key, $n_b = 5, P_m = (6, 8)$, and chooses the random k value as 2.	10	CO2	BL3

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. 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: A – 01234567 B – 89abcdef C – fedcba98 D – 76543210	5 5	CO3	BL4
5.	Using the ElGamal Digital signature scheme, User A chose p=13, q=2, private key X_A = 3, H(m) = 11, k = 5. He announces the global componenets publicily. (i) Find the publich key Y_A (ii) How user A does the signing process to compute (S1, S2)? (iii) How user B does the verification process?	 2 4 4	CO3	BL4

1) a) $e = 13$

$n = 77$

$P = 11, \quad Q = 7$

$\phi(n) = (P-1) \times (Q-1)$

$= 10 \times 6\cancel{0}$

$\phi(n) = 60$

$C = 20$

$PT = C^{D} \bmod n$

$(D \times E) \bmod \phi(n) = \underline{1}$

$(D \times 13) \bmod 60 = \underline{1}$

$13^{-1} \bmod 60$

$\gcd(13, 60) = 1$

q	r_1	r_2	r	t_1	t_2	t
4	60	13	8	0	1	-4
1	13	8	5	1	-4	5
1	8	5	3	-4	5	-9
1	5	3	2	5	-9	14
1	3	2	1	-9	14	-23
	2	1		14	-23	

2

$t = t_1 - t_2 \times q$

$= 0 - 1 \times 4$

$t = -4$

$t = 1 - (-4) \times 1$

$= 1 + 4$

$t = 5$

$t = -4 - 5 \times 1$

$= -9$

$t = 5 - (-9) \times 1$

$t = 14$

$t = -9 - 14 \times 1$

$= -23$

$1 \overline{)2}$ 2
$\underline{2}$
0

q	r_1	r_2	r	t_1	t_2	t
2	2	1	0	14	-23	-32
	1	0		-23	-32	

③

$t = 14 - (-23) \times 2$

$t = -32$

$D = -23 + 60$

$D = 37$

$PT = 20^{37} \bmod 77$

~~$PT = 20^{18} \cdot 20^{19} \bmod 77$~~

$PT = 20^{10} \cdot 20^{10} \cdot 20^{10} \cdot 20^{7} \bmod 77$

$= 54 \cdot 54 \cdot 54 \cdot 48 \bmod 77$

$PT = 29$

1) b) $p = 11$, $g = 2$

$X_A = 9$ $X_B = 4$

$A = g^{x_a} \bmod p$

$B = g^{x_b} \bmod p$

$K1 = B^{x_a} \bmod p$

$K2 = A^{x_b} \bmod p$

$A = 2^9 \bmod 11$

$\boxed{A = 6}$

$B = 2^4 \bmod 11$

$\boxed{B = 5}$

$K1 = 5^9 \bmod 11$ | $K2 = 6^4 \bmod 11$

$K1 = 9$ | $K2 = 9$

5) $P = 13, \; q = 2$ (5)

$X_A = 3 \quad m = 11 \quad K = 5$

1. Key Generation

$X_A = 3$

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

$= 2^3 \bmod 13$

$\boxed{Y_A = 8}$

2. Signing

$m = 11$

$K = 5$

a) $S1 = q^K \bmod P$

$= 2^5 \bmod 13$

$S1 = 6$

b) $K^{-1} \bmod P-1$

$5^{-1} \bmod 12$

q	r_1	r_2	r	t_1	t_2	t
2	12	5	2	0	1	-2
2	5	2	1	1	-2	5
2	2	1	0	-2	5	-12
	1	0		5	-12	

$t = t_1 - t_2 \times q$

$= 0 - 1 \times 2$

$t = -2$

$t = 1 - (-2) \times 2$

$= 1 - (-4)$

$t = 5$

$t = -2 - 5 \times 2$

$= -2 - 10$

$t = -12$

$5^{-1} \bmod 12 = 5$

⑦

$$S2 = \left[k^{-1}(m - X_A S1)\right] \bmod p-1$$

$$\left[5 \cdot (11 - 9 \cdot 6)\right] \bmod 12$$

$$S2 = \left[5 \cdot (11 - 54)\right] \bmod 12$$

$$= \left[5 \times (-43)\right] \bmod 12$$

$$= -215 \bmod 12$$

$$= 12 - (215 \bmod 12)$$

$$12 - 11$$

$$= \cancel{10-5}$$

$$= 1$$

$$\cancel{S2 = 5}$$

$$(S1, S2) = (6, 1)$$

$$\cancel{(S1, S2)} = \cancel{(6, 5)}$$

3. Verification

$$V_1 = q^m \bmod p$$

$$= 2^{11} \bmod 13$$

$$V_1 = 7$$

$$V2 = (Y_A)^{S1} \cdot (S1)^{S2} \bmod P$$

$$= 8^{6} \cdot 6^{1} \bmod 13$$

$$= 12 \cdot 6 \bmod 13$$

~~V2 = 11~~

$V2 = 7$

$$\boxed{V1 = V2}$$

4(a) Message = 4000 bits

Padding Bits

64 bits less than the multiple of 512

$512 \times 8 = 4096$

$4096 - 64 = 4032$

padding Bits = 32 bits

$4096 / 512 = 8$ 512-bit block

2(a) $q = 157$ $\alpha = 5$

i) $Y_B = 10$ $k = 3$ $M = 9$

$K = (Y_B)^k \bmod q$

$= 10^3 \bmod 157$

$K = 58$

$C1 = \alpha^k \bmod q$

$= 5^3 \bmod 157$

$C1 = 125$

$C2 = K.M \bmod q$

$= 58.9 \bmod 157$

$C2 = 51$

$(C1, C2) = (125, 51)$

2(b)

$q = 157 \quad \alpha = 5$

$Y_B = 10 \quad k = ? \quad M = 9$

$C = (25, C2) \quad C2 = ?$

$21 = 5^{k} \bmod 157$

$\boxed{k = 73}$

$C2 = K \cdot M \bmod q$

$K = 10^{73} \bmod 157$

$\boxed{K = 122}$

$C2 = 122 \cdot 9 \bmod 157$

$C2 = 156$

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

$$P_b = n_b * G = 5 * (5,5)$$

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 $5 * G$,

$$5 * G = 3 * G + 2 * G = (11,11) + (7,4) \tag{20}$$

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,

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

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

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

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 $18^{-1}\ mod\ 13$,

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

$$= 1 * 8\ mod\ 13 = 8$$

So, we got,

$$\lambda = 8\ ,\ X = 5 \text{ and } Y = 5$$

Now, we find X_3 and Y_3,

Finding X_3,

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

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

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 $k * P_b$, we can compute the 2nd part of 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

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

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

$$= 24 \, mod \, 13 = 11$$

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 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)	$(b \wedge c) \vee (b \wedge d)$
2	G(b, c, d)	$(b \wedge d) \vee (c \wedge d)$
3	H(b, c, d)	$b \oplus c \oplus d$
4	I(b, c, d)	$c \oplus (b \vee d)$

For F

For F

B = 1000 1001 1010 1011 1100 1101 1110 1111

C = 1111 1110 1101 1100 1011 1010 1001 1000 AND

1000 1000 1000 1000 1000 1000 1000 1000

$B \wedge C =$

$\neg B =$ 0111 0110 0101 0100 0011 0010 0001 0000

D = 0111 0110 0101 0100 0011 0010 0001 0000

0111 0110 0101 0100 0011 0010 0001 0000

$\neg B \wedge D =$

$B \wedge C =$ 1000 1000 1000 1000 1000 1000 1000 1000

F = 1111 1110 1101 1100 1011 1010 1001 1000

F E D C B A 9 8

So, final F = FEDCBA98

For G

For G

B = 1000 1001 1010 1011 1100 1101 1110 1111 AND

D = 0111 0110 0101 0100 0011 0010 0001 0000

0000 0000 0000 0000 0000 0000 0000 0000

$B \wedge D =$

C = 1111 1110 1101 1100 1011 1010 1001 1000 AND

$\neg D$ = 1000 1001 1010 1011 1100 1101 1110 1111

$C \wedge \neg D =$ 1000 1000 1000 1000 1000 1000 1000 1000

C∧¬D = 1000 1000 1000 1000 1000 1000 1000 1000
B∧D = 0000 0000 0000 0000 0000 0000 0000 0000 (OR)

G = 1000 1000 1000 1000 1000 1000 1000 1000

G = 8 8 8 8 8 8 8 8

For H

B: 1000 1001 1010 1011 1100 1101 1110 1111 ⊕ XOR

C: 1111 1110 1101 1100 1011 1010 1001 1000

B⊕C: 0111 0111 0111 0111 0111 0111 0111 0111 ⊕ XOR

D: 0111 0110 0101 0100 0011 0010 0001 0000

H: 0000 0001 0010 0011 0100 0101 0110 0111

0 1 2 3 4 5 6 7

H = 0 1 2 3 4 5 6 7

For I

B = 1000 1001 1010 1011 1100 1101 1110 1111

¬D = 1000 1001 1010 1011 1100 1101 1110 1111

B∨¬D = 1000 1001 1010 1011 1100 1101 1110 1111 ⊕

C = 1111 1110 1101 1100 1011 1010 1001 1000

I: 0111 0111 0111 0111 0111 0111 0111 0111

I = ~~8 8 8 8 8 8 8 8~~ 7 7 7 7 7 7 7 7

So, finally, we got:

F = FEDC BA98

G = 8888 8888

H = 0123 4567

I = 7777 7777