COLLEGE OF ENGINEERING PUNE (COEP)

(An Autonomous Institute of Government of Maharashtra)

END Semester Examination

Programme: B. Tech **Semester: VII**
Course Code: CT-22003 **Course Name: Cryptography and Network Security**
Branch: Computer Engineering **Academic Year: 2024-25**
Duration: 3 Hr. **Max Marks: 60**
Student PRN No: □□□□□□□□□

Instructions:

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of stationery, calculator etc. not allowed.
5. Write your PRN Number on Question Paper.

Marks **CO** **PO**

Q.1. A. Fill in the blanks and **Re-write** the complete sentence with correct answer: **(6)** **CO-1, CO-2, CO-3, CO-4, CO-5,** **a, e, g,**

1. The first step in MD5 algorithm is ___________.

   a. Padding b. add length

   c. divide into subblocks d. initial permutation

2. The problem with Diffie-Hellman Key Agreement Protocol is ________

   a. too short keys b. lack of security

   c. failure to agree on the key d. person in the middle attack

3. __________ is anything that can cause harm.

   a. Vulnerability b. Phish

   c. Threat d. Spoof

4. In Triple DES, we can use ___ or ____ keys.

   a. 1 or 2 b. 3 or more

   c. 1 or more d. 2 or 3

5. The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext the scheme is known as ____________.

   a) Confusion b) Diffusion

   c) Error Propagation d) Avalanche Effect

6. What is the multiplicative inverse of 5 (mod 101)?

   a. 5^{99} b. 5^{100}

   c. 21^{49} d. Can't be determined

B. Illustrate the various steps used in Man-in-the-Middle Attack. What is replay attack? What are the different types of replay attacks? Explain each in brief. Also discuss the counter measures for these attacks. (6)

Q.2. A. Explain the working of PGP. Your answer should include block diagram, need of PGP, and working of PGP and encryption applications of PGP. (6)

CO-1, b, e,
CO-2, c
CO-4,

OR

A. In Secure Socket Layer (SSL) protocol there are different protocols. One of these protocols Handshake protocol. In this protocol a logical connection is initiated between the client and server. What are the fields of client_hello and server_hello message? Discuss the content/importance of each field. (6)

B. Sachin's friend posts the RSA public key (n = 3551; e = 1565), hoping for secret messages from his friends. One of his friends sent him a magic number 67 to him. What is the private key of Sachin's friend? (6)

Q.3. A. For the following questions, assume the use of the field F_{2^3}. The field is described here using polynomial representation with the irreducible polynomial $x^3 + x + 1$. The generator for the field is $g = (010)$, and the powers of g are: $g^1 = (010)$ $g^2 = (100)$ $g^3 = (011)$ $g^4 = (110)$ $g^5 = (111)$ $g^6 = (101)$ $g^7 = (001) = 1$ (6)

CO-3, a, e,
CO-4, f g,
CO-5

i) Does the elliptic curve equation $y^2 + xy = x^3 + g^5x^2 + g^6$ define a group over F_{2^3}?

ii) Do the points $P(g^3, g^6)$ and $Q(g^5, g^2)$ lie on the elliptic curve $y^2 + xy = x^3 + g^2x^2 + g^6$ over F_{2^3}?

iii) What are the negatives of the following elliptic curve points over F_{2^3}? $P(g^3,g^6)$ $Q(g,0)$ $R(0,g^3)$

iv) In the elliptic curve group defined by $y^2 + xy = x^3 + g^2x^2 + g^6$ over F_{2^3}, what is P + Q if $P = (g^2,g^6)$ and $Q = (g^5,g^5)$?

v) In the elliptic curve group defined by $y^2 + xy = x^3 + g^2x^2 + g^6$ over F_{2^3}, what is 2P if $P = (g^3, g^4)$?

OR

A. Illustrate the procedure for padding in Message Digest 5 (MD5) with proper example. If the message is of 3012 bits size, how many numbers of bits are required for padding this message? What are the padding bits? List the properties of Hash Functions. (6)

B. Answer the following: (6)

a) Using Fermat's little theorem find the last two digits of 171^{401} mod 100

b) Calculate 67^{-1} (*mod 119*) and use this to calculate $\frac{43}{67}$ (*mod* 119).

c) How many numbers are relatively prime to 25.

d) Solve $9x \equiv 1 \pmod{7}$

Q.4. A. Calculate the K^{-1} required during decryption of Hill Cipher technique, where the K matrix is given by the key "GYBNQKURP" (3) CO-1, CO-3, CO-4, a, d, f

B. Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root $\alpha = 2$. (3)

a. Show that 2 is a primitive root of 11. 4

b. If user A has public key $Y_A = 9$, what is A's private key X_A? 2

c. If user B has public key $Y_B = 3$, what is the shared secret key K, shared with A? 4

C. Calculate the digital signature using following data: (6)
Global public key values are 29 and 9, h =7,
Users Private key = 5 and K =7, $K^{-1} = 5$,

Find the public key and the digital signature for the message whose message digest is 53.

Q.5. A. Perform AES mix column transformation for following and show your calculations. (6) CO-2, b, c, e,

$$\text{Rcon=} \begin{matrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{matrix} \quad \text{State column =} \begin{matrix} 87 \\ 6E \\ 46 \\ A6 \end{matrix}$$

B. Six professors begin lectures on Monday, Tuesday, Wednesday, Thursday, Friday and Saturday, and announce their intentions of lecturing at intervals of 2, 3, 4, 1, 6, 5 days respectively. The regulations of the University forbid Sunday lectures (so that Sunday lectures must be omitted). When will all six professors find themselves compelled to omit a lecture? (5)