BE INFO TECH 3rd YEAR 2nd SEMESTER EXAMINATION 2025

Information Security

Time: 3 Hours Full Marks: 100

Answer All Questions

[Please show all intermediate steps clearly and elaborately. Do not skip any steps]

1.a) Differentiate among Security Attack, Security Mechanism and Security Service.

b) Illustrate how one can easily create a Key for Transposition Cipher which can be remembered very easily. (5+5) **[CO1]**

2.a) Using Extended Euclidean Algorithm, find the multiplicative inverse of 11 in Z_{46}.

b) How many primitive elements are there in the group (Z^*_{41}, X)? Is 14 a primitive element of this group? Justify your answer.

c) Illustrate Square and Multiply algorithm to find Discrete Logarithm. (3+(1+1+2)+3) **[CO2]**

3.a) Illustrate the concept of S-Box .

b) Illustrate the MixColumns phase in AES during the encryption phase. The constant Matrix is given below.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

c) Using a proper diagram, explain the ShiftRows phase in AES during the encryption. (4+3+3) **[CO3]**

4.a) With regard to the RC4 Stream Cipher, write down the value of the first 10 bytes of S and T vectors. Assume the Key is "Key".

b) Illustrate your understanding about CFB mode. How can CFB mode be used as Stream Cipher?

c) Write two differences between the CBC and CTR mode. (3+(3+2)+2) **[CO3]**

5.a) Using Color Arithmetic, explain Diffie-Hellman Key Exchange Algorithm.

b) Using relevant numerical examples, explain Rabin Cryptosystem.

c) With regard to the RSA algorithm, Illustrate your understanding about Chosen-Ciphertext Attacks.

(3+3+4) **[CO4]**

6.a) For the Short-Weierstrass Elliptic Curve, doubling of a point is given by the formulae as shown below.

$$x_R = l^2 - 2x_P$$
$$y_R = l(x_P - x_R) - y_P$$
$$\text{where, } l = (3x_P^2 + a)/2y_p.$$

Here, the point to be doubled is P with coordinate (x_P, y_P); and the doubled point is R with coordinate (x_R, y_R). Using the above formula, double the following points for the curve E_{23} (10, 11).

i) (5,18); ii) (4,0); iii) (16,9); iv) (22,0).

b) For the elliptic curve E_{23} (10, 11), find the order of the four points mentioned below. Please note that the Curve Order is 16.

i) (5,5); ii) (4,0); iii) (11,7); iv) (20,0).

c) For a certain Elliptic Curve (over finite field), the curve order is prime. So, we can safely assume that all points for this curve are the generator points. True or False? Justify your answer.

(4+4+2) **[CO4]**

7.a) For a Hash Function, the security refers to the fact that a birthday attack on a message digest of size n produces a collision with a workfactor of approximately $2^{n/2}$. Explain this.

b) Discuss the differences between MDC and MAC. Explain the scenarios with examples, where they will be helpful.

c) Discuss the differences between HMAC and CMAC. (3+4+3) **[CO5]**

8.a) When it comes to sending messages between two parties, how Public Key Cryptosystems can be used for Confidentiality, Authentication and Signature? Explain it with a proper diagram.

b) Differentiate between Message Authentication and Entity Authentication.

c) With the help of a proper diagram explain the Challenge-Response Protocols using a Public Key Cryptosystems. (3+2+5) **[CO5]**

9.a) Illustrate and Explain a Simple Protocol by which Alice and Bob can exchange messages using a symmetric key cryptosystem by taking the help of a KDC.

b) Illustrate and Explain Kerberos Protocol.

c) Illustrate and Explain the format of a X.509 Certificate.

(2+5+3) **[CO5]**

10.a) Rather than using a usual text encryption technique, why do we need separate schemes for image encryption?

b) List down the names of at least 8 Scan Patterns. Explain one of them.

c) What is Histogram Analysis?

(2+(4+2)+2) **[CO6]**