| Reg. No. | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| Question Paper Code | 13440 |
|---|---|

**B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2025**

Seventh Semester

**Information Technology**

(Common to Computer Science and Engineering)

**20ITPC701 - CRYPTOGRAPHY AND NETWORK SECURITY**

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

**PART - A (MCQ) (10 × 1 = 10 Marks)**

Answer ALL Questions

| | | Marks | K – Level | CO |
|---|---|---|---|---|
| 1. | What is the main purpose of using a product cryptosystem in encryption?<br>(a) To speed up the encryption process<br>(b) To combine multiple transformations, like substitution and permutation, for stronger security<br>(c) To store encryption keys in a database<br>(d) To compress data before encryption | 1 | K1 | CO1 |
| 2. | If the message "HELLOWORLD" is encrypted using the Rail fence technique with 2 rails, what will be the ciphertext?<br>(a) HLOOLELWRD (b) HELOWORLD (c) HWEOLLRLOD (d) None of the above | 1 | K2 | CO1 |
| 3. | Find the result of the following operation: −18 mod 14<br>(a) -4 (b) -18 (c) 1 (d) 10 | 1 | K2 | CO2 |
| 4. | Which of the following is true for a finite field?<br>(a) Every element has a multiplicative inverse (b) Division is not allowed<br>(c) The number of elements must be even (d) Addition is not associative | 1 | K1 | CO2 |
| 5. | What is the main advantage of Elliptic Curve Cryptography (ECC) over RSA?<br>(a) ECC provides equal security with smaller key sizes, reducing processing overhead<br>(b) ECC requires more memory than RSA<br>(c) ECC is easier to implement than RSA<br>(d) ECC supports only digital signatures, not encryption | 1 | K2 | CO3 |
| 6. | Find the value of φ(10)<br>(a) 10 (b) 9 (c) 4 (d) 1 | 1 | K2 | CO3 |
| 7. | Identify the number of key(s) used to encrypt and decrypt the data, in symmetric encryption<br>(a) Two keys (b) One key (c) No key (d) Three keys | 1 | K2 | CO4 |
| 8. | If an attacker gains access to the AES encryption key used in a system, what is the most serious consequence?<br>(a) They can only read file names, not file content<br>(b) They can reset the encryption algorithm<br>(c) They must still guess the password to decrypt the data<br>(d) They can decrypt all data encrypted with that key | 1 | K2 | CO4 |
| 9. | Who issues an X.509 certificate?<br>(a) Internet Service Provider (ISP) (b) Certificate authority (CA)<br>(c) Firewall administrator (d) Web browser | 1 | K1 | CO5 |
| 10. | What does a packet filtering firewall do?<br>(a) It encrypts all outgoing emails<br>(b) It scans computers for viruses<br>(c) It checks each IP packet against rules and allows or blocks it<br>(d) It stores all incoming packets for later review | 1 | K1 | CO6 |

**PART - B (12 × 2 = 24 Marks)**

Answer ALL Questions

| | | Marks | K – Level | CO |
|---|---|---|---|---|
| 11. | Construct a 5 x 5 key matrix for the keyword 'communication' using playfair cipher method. | 2 | K2 | CO1 |
| 12. | Compare active attack and passive attack. | 2 | K2 | CO1 |

| | | | | | |
|---|---|---|---|---|---|
| 13. | Define an algebraic structure. | | 2 | K1 | CO2 |
| 14. | Summarize the key properties of modular arithmetic. | | 2 | K2 | CO2 |
| 15. | List different techniques used for the distribution of public keys. | | 2 | K1 | CO3 |
| 16. | Find the result of $6^{10}$ mod 11. | | 2 | K2 | CO3 |
| 17. | Differentiate between stream cipher and block cipher. | | 2 | K2 | CO4 |
| 18. | What are the four main stages in each round of AES algorithm? | | 2 | K1 | CO4 |
| 19. | Distinguish between message authentication and entity authentication. | | 2 | K2 | CO5 |
| 20. | Outline some advantages and disadvantages of using long passwords. | | 2 | K2 | CO5 |
| 21. | Classify three types of intruders. | | 2 | K2 | CO6 |
| 22. | What is Transport Layer Security (TLS)? | | 2 | K1 | CO6 |

## PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

| | | | | | | |
|---|---|---|---|---|---|---|
| 23. | a) | (i) | With a block diagram explain conventional encryption model and entities involved. | 6 | K2 | CO1 |
| | | (ii) | Explain Steganography and list its uses. | 5 | K2 | CO1 |
| | | | **OR** | | | |
| | b) | | Summarize about security services defined in X.800. | 11 | K2 | CO1 |
| 24. | a) | | Use the extended Euclidean algorithm to find the modular multiplicative inverse of 1234 mod 4321. | 11 | K3 | CO2 |
| | | | **OR** | | | |
| | b) | | Utilize the concepts of groups, rings, and fields to explain their importance in cryptographic algorithms. | 11 | K3 | CO2 |
| 25. | a) | | Write RSA algorithm. Perform encryption and decryption using the RSA algorithm for the following: p = 7, q = 11, e =13, M = 5. | 11 | K3 | CO3 |
| | | | **OR** | | | |
| | b) | | Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 23 and a primitive root $\alpha = 5$ .<br>(i) If Bob has a public key $Y_B = 1\ 0$ , what is Bob's private key $Y_B$?<br>(ii) If Alice has a public key $Y_A = 8$ , what is the shared key K with Bob?<br>(iii) Show that 5 is a primitive root of 23. | 11 | K3 | CO3 |
| 26. | a) | | Examine the encryption and decryption processes of Simplified DES (S-DES) in detail, illustrating the results at each step. | 11 | K4 | CO4 |
| | | | **OR** | | | |
| | b) | | Analyze the RC4 stream cipher in detail by presenting its working mechanism, pseudocode, and a supporting diagram. | 11 | K4 | CO4 |
| 27. | a) | | Identify the main components of the Kerberos authentication system. Explain the role and purpose of the following two bi-directional exchanges involved in the Kerberos authentication process with a diagram:<br>(i) Between the client and the Key Distribution Center (KDC), the Ticket Granting Service (TGS)<br>(ii) Between the client and the application server. | 11 | K3 | CO5 |
| | | | **OR** | | | |
| | b) | | Apply the Digital Signature Algorithm (DSA) to show how it helps protect digital messages. Also, write the basic steps to create and verify a digital signature using DSA. | 11 | K3 | CO5 |
| 28. | a) | | Analyze threats to a wireless network by examining their nature and impact on system security. | 11 | K4 | CO6 |
| | | | **OR** | | | |
| | b) | | Categorize the key services offered by Pretty Good Privacy (PGP), and illustrate each with examples. | 11 | K4 | CO6 |