Hall Ticket No | | | | | | | | | | |

Question Paper Code: AITC11

INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)
Dundigal-500043, Hyderabad

B.Tech V SEMESTER END EXAMINATIONS (REGULAR/ SUPPLEMENTARY) - FEBRUARY 2024
Regulation: UG20

CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 Hours **(INFORMATION TECHNOLOGY)** **Max Marks: 70**

Answer ALL questions in Module I and II
Answer ONE out of two questions in Modules III, IV and V
All Questions Carry Equal Marks
All parts of the question must be answered in one place only

MODULE – I

1. (a) Write short notes on security attacks. Differentiate between symmetric and asymmetric key cryptography. [BL: Understand| CO: 1|Marks: 7]

   (b) Apply the column and row transposition techniques to encrypt the message "attack postponed until two am". The column transposition encryption key is 3 4 2 1 5 6 7 and row transposition key is 4 2 3 1. Find the decryption keys and decrypt the ciphertext to get back the plaintext message. [BL: Apply| CO: 1|Marks: 7]

MODULE – II

2. (a) Draw the general structure of data encryption standard (DES) with encryption process. [BL: Understand| CO: 2|Marks: 7]

   (b) Perform encryption and decryption using RSA algorithm for the following
   P=7; q=11; e=17; M=8 [BL: Apply| CO: 2|Marks: 7]

MODULE – III

3. (a) Discuss about the objectives of hash-based message authentication code (HMAC) and it security features. [BL: Understand| CO: 3|Marks: 7]

   (b) How digital signature differs from authentication protocols? Discuss clearly digital signature algorithm. [BL: Understand| CO: 3|Marks: 7]

4. (a) Classify various types of attacks that are addressed by message authentication. How is the encryption key generated from password in Kerberos? [BL: Understand| CO: 4|Marks: 7]

   (b) What is simple and secure authentication? Interpret what characters are needed in a secure hash function? [BL: Understand| CO: 4|Marks: 7]

MODULE – IV

5. (a) Why pretty good privacy (PGP) is open source? Explain the services that are provided in PGP. [BL: Understand| CO: 5|Marks: 7]

   (b) Develop step-by-step overview of the process involved in transmitting a PGP-encrypted message. Include key generation, encryption, and the use of digital signatures. [BL: Apply| CO: 5|Marks: 7]

6. (a) How does secure/multipurpose internet mail extension S/MIME address email security problems? Elucidate. [BL: Understand| CO: 5|Marks: 7]

   (b) Differentiate between the authentication header (AH) and encapsulating security payload (ESP). [BL: Understand| CO: 5|Marks: 7]

MODULE – V

7. (a) List out design goals for a firewall. Outline the steps involved in secure electronic transaction (SET) transaction. [BL: Understand| CO: 6|Marks: 7]

   (b) Write three benefits that can be provided by an intrusion. Elucidate how statistical anomaly detection is different from rule based intrusion? [BL: Understand| CO: 6|Marks: 7]

8. (a) How do firewalls complement other security measures against intrusions? Illustrate the different phases of a computer virus's lifecycle. [BL: Understand| CO: 6|Marks: 7]

   (b) Design a secure cryptographic solution that should authenticate the origin of the payment instructions to prevent unauthorized transactions. [BL: Apply| CO: 6|Marks: 7]

– ○ ○ ◯ ○ ○ –