Hall Ticket No | | | | | | | | | | | Question Paper Code:AITC11

INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)
(Dundigal-500043, Hyderabad)

B.Tech V SEMESTER END EXAMINATIONS (REGULAR) - DECEMBER 2022
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) What are the basic fundamental requirements of network security? Explain all the fundamental requirements for network and computer security. [BL: Understand| CO: 1|Marks: 7]

   (b) Make use of hill cipher to decrypt the word ATTACK where the key is [BL: Apply| CO: 1|Marks: 7]

$$\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$$

MODULE – II

2. (a) Demonstrate the analytic and timing attack in DES, also give the requirements of key size to strengthen the DES algorithm [BL: Understand| CO: 2|Marks: 7]

   (b) Use RSA diffie hellman key exchange technique with a common prime q=71 and primitive root α=7.

   i) If user A has private key X_A=5, what is A's public key Y_A?

   ii) If user B has private key X_B=5, what is B's public key Y_B?

   iii) What is the shared secret key? [BL: Apply| CO: 2|Marks: 7]

MODULE – III

3. (a) List and explain the message authentication requirements with respect to network security. [BL: Understand| CO: 3|Marks: 7]

   (b) Outline the structure and format of X.509 certificate required for key management and distribution with a neat figure. [BL: Apply| CO: 3|Marks: 7]

4. (a) Explain the Kerberos version 4 overview with all the client/server authentication phases to obtain the services. [BL: Understand| CO: 4|Marks: 7]

   (b) Apply the hash-based message authentication code (HMAC) algorithm for message authentication and explain with examples. [BL: Apply| CO: 4|Marks: 7]

MODULE – IV

5. (a) Describe in detail about transport mode versus tunnel mode encryption required in IP security and explain in detail. [BL: Understand| CO: 5|Marks: 7]

   (b) Identify the top level format of an encapsulating security payload(ESP) packet required for IP security and explain in detail. [BL: Apply| CO: 5|Marks: 7]

6. (a) Discuss about S/MIME message content types and also describe the services provided by S/MIME. [BL: Understand| CO: 5|Marks: 7]

   (b) Utilize PGP for confidentiality and authentication in electronic mail security and discuss with example. [BL: Apply| CO: 5|Marks: 7]

MODULE – V

7. (a) What is cross site scripting ? Explain the launching of the cross site scripting attack. [BL: Understand| CO: 6|Marks: 7]

   (b) Which are the three classes of intruders? Choose the different approaches for intrusion detection system and explain them. [BL: Apply| CO: 6|Marks: 7]

8. (a) Explain the different types of threats and counter measures for web security. [BL: Understand| CO: 6|Marks: 7]

   (b) Identify the secure socket layer (SSL) record protocol operation for network and internet security and discuss SSL record protocal in detail. [BL: Apply| CO: 6|Marks: 7]