Hall Ticket No | | | | | | | | | | | Question Paper Code: AITB22

INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)

B.Tech V Semester End Examinations (Regular), February – 2021
Regulation: IARE–R18

INFORMATION SECURITY

Time: 3 Hours **(CSE | IT)** **Max Marks: 70**

Answer any Four Questions from Part A
Answer any Five Questions from Part B

PART – A

1. Explain the different types of security services in detail. **[5M]**
2. Elucidate in detail about elliptic curve cryptography key distribution. **[5M]**
3. Discuss in detail about Knapsack algorithm with an example. **[5M]**
4. Explain about the general format for PGP message. **[5M]**
5. Give informative notes on transport layer security. **[5M]**
6. What is steganography? Briefly explain any three techniques used. **[5M]**
7. Compare public key and private key cryptography and list various algorithms for each. **[5M]**
8. List and explain the objectives of HMAC and its security features. **[5M]**

PART – B

9. With a neat block diagram, explain the network security model and the important parameters associated with it. **[10M]**
10. Define Rail fence technique. Convert the given text "This is a secret message" into cipher text using rail fence technique. **[10M]**
11. Explain the following modes of operation in block cipher
    i) Electronic code book
    ii) Cipher block chain mode **[10M]**
12. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6
    i)What is the public key of Alice?
    ii)What is the public key of Bob?
    iii) what is the secret key they exchanged? **[10M]**
13. Discuss in detail about following entity authentication mechanisms
    i)Using password
    ii)Using digital signature **[10M]**
14. Describe the roles of the different servers in Kerberos protocol.How does the user get authenticated to the different servers? **[10M]**
15. List out the pros and cons of transport and tunnel mode. Illustrate. **[10M]**
16. Discuss about encapsulating security payload of IP. **[10M]**
17. Elucidate the following
    i) Firewall design principles.
    ii) Types of firewalls. **[10M]**
18. Write short notes on intruders and elaborate the concept of intrusion detection. **[10M]**

– ○○◯○○ –