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

Question Paper Code: ACS013

INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

B.Tech VI Semester End Examinations (Regular), November– 2020

Regulation: IARE–R16

INFORMATION SECURITY

Time: 2 Hours **(CSE)** **Max Marks: 70**

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

PART – A

1. Explain one-time pad substitution cipher with example. **[5M]**
2. Write the ECC-Diffie Hellman key exchange algorithm. **[5M]**
3. Briefly explain about knapsack algorithm. **[5M]**
4. Illustrate the operational description of PGP. **[5M]**
5. Write the differences between SSL and TLS. **[5M]**
6. Briefly discuss about a model for network security. **[5M]**
7. Explain in detail about advanced encryption standard (AES) algorithm. **[5M]**
8. Write the Kerberos version 4 authentication dialogue. **[5M]**

PART – B

9. Suppose m=6 and the keyword is CIPHER. This corresponds to the numerical equivalent K=(2, 8, 15, 7 , 4, 17). Consider the plain text is 'thiscryptosystemisnotsecure'. What is the corresponding cipher text using Vigenere cipher method. **[10M]**
10. Write short notes on i) confidentiality ii) Authentication iii) Integrity iv) Non-Repudiation **[10M]**
11. Explain electronic code book mode(EBC) and cipher block chain mode (CBC) modes of operation in DES with neat diagrams. **[10M]**
12. Perform encryption and decryption using the RSA algorithm for the following: p = 17; q = 11, e = 7; M = 88. **[10M]**
13. What are the improvements in Kerberos version five over version four? **[10M]**
14. What is Realm? Briefly explain about Kerberos realm concept. Briefly explain about X.509 public-key certificates. **[10M]**
15. Sketch the IPSec ESP format and explain the functionality of ESP in transport mode. **[10M]**
16. Explain the fields present in the frame format of ISAKMP Header and write the ISAKMP exchange types. **[10M]**
17. Draw the SSL protocol stack format and explain various phases of SSL handshake protocol. **[10M]**
18. List the characteristics of a firewall and design goals and describe about packet filtering firewall. **[10M]**