Hall Ticket No □□□□□□□□□□ Question Paper Code: ACS013

INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

B.Tech VI Semester End Examinations (Regular) - May, 2019

Regulation: IARE – R16

INFORMATION SECURITY

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

Answer ONE Question from each Unit
All Questions Carry Equal Marks
All parts of the question must be answered in one place only

UNIT – I

1. (a) Explain one-time pad substitution cipher with example. Briefly discuss about a model for Network Security. **[7M]**

   (b) 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 Polygram substitution cipher method.

2. (a) Write short Notes on
   i. Confidentiality
   ii. Authentication
   iii. Integrity
   iv. Non-Repudiation **[7M]**

   (b) Convert the following plain text message P=”cryptography provides high security” into cipher text by using simple columnar transposition basic technique with multiple rounds. **[7M]**

UNIT – II

3. (a) Explain Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes of operation in DES Algorithm the with neat diagrams. **[7M]**

   (b) Perform encryption and decryption using the RSA algorithm for the following:
   $p = 17; q = 11, e = 7; M = 88.$ **[7M]**

4. (a) Explain in detail about Advanced Encryption Standard (AES) Algorithm with neat diagram. **[7M]**

   (b) If a bit error occurs in the transmission of a cipher text character in 8-bit Cipher Feed Back (CFB) mode, how far does the error propagate? **[7M]**

UNIT – III

5. (a) What are the improvements in Kerberos version 5 version 4? Briefly explain about Knapsack algorithm. **[7M]**

   (b) Explain why has there been an interest in developing a message authentication code derived from a cryptographic hash function as opposed to one derived from a symmetric cipher? **[7M]**

6. (a) Define Realm. And briefly explain about Kerberos Realm concept. **[7M]**

   (b) Describe the differences between MD4 and MD5. Do you think that MD5 is stronger than MD4, and why? **[7M]**

UNIT – IV

7. (a) Illustrate the operational description of PGP. Write the Kerberos version 4 authentication dialogue. **[7M]**

   (b) Explain of MIME specification with an example. Justify why S/MIME is a security enhancement to MIME internet email format standard? **[7M]**

8. (a) Explain the fields present in the frame format of ISAKMP Header and write the ISAKMP exchange types. **[7M]**

   (b) Generalize why in spite of symmetric key, public key and private key, uses three separate requirements. What are those and explain why are used? **[7M]**

UNIT – V

9. (a) Draw the SSL protocol stack format and explain various phases of SSL handshake protocol. Write the differences between SSL and TLS. **[7M]**

   (b) In SSL and TLS, why is there a separate change cipher Spec protocol rather than including a change cipher-Spec message in the Handshake protocol? **[7M]**

10. (a) List the characteristics of a firewall and explain its design goals. Describe about packet filtering firewall.

    [7M]

    (b) Write short notes on:

    i. Backdoor

    ii. Logic Bomb

    iii Trojan Horses

    iv. Worms.

    [7M]

– ○ ○ ◯ ○ ○ –