Reg. No. : | | | | | | | | | | |

Question Paper Code: 31724

B.E. / B.Tech. DEGREE EXAMINATION, NOV 2016

Seventh Semester

Computer Science and Engineering

01UCS704 - FUNDAMENTALS OF INFORMATION SECURITY

(Regulation 2013)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1. What is access control matrix?
2. List the different security policies and types of access control.
3. Explain how the avalanche effect is achieved in DES.
4. Does Diffie-Hellman key exchange provide security against man-in-the middle attack? Justify your answer?
5. List the requirements of MAC functions.
6. Distinguish between direct and arbitrated digital signature schemes.
7. What is the difference between vulnerability and exposure?
8. Differentiate between rule-based anomaly detection and rule-based penetration identification.
9. Can routers and bridges be used as firewalls? How?
10. Define application gateway.

PART - B (5 x 16 = 80 Marks)

11. (a) (i) Explain in detail about access control matrix with examples. (10)

(ii) Discuss about clinical information systems security policy. (6)

Or

(b) (i) Briefly explain the components of an information system and their security. (8)

(ii) Explain in detail about clark wilson integrity model and lower water mark policy. (8)

12. (a) (i) How AES is used for encryption/decryption? Explain with example. (8)

(ii) Discuss in detail about CBC and OFB mode of DES operations. (8)

Or

(b) (i) Explain in detail about public key cryptosystem secrecy and authentication with a neat diagram. (8)

(ii) In RSA cryptosystem with parameters $p=11$, $q=13$, $e=11$, find the public key, private key and ciphertext corresponding to the plaintext $m=7$. (8)

13. (a) (i) Explain the MD5 message digest algorithm by giving suitable diagrams for message digest generation and message processing of 512 bit block and MD5operation. (10)

(ii) Discuss about the process of signature verification in DSS. (6)

Or

(b) Consider an ElGamal scheme with a common prime $q=11$ and primitive root $\acute{a}=2$, $k=2$.

(i) If *A* has public key $XA=5$, What is *A*'s private key *YA*

(ii) If user *B* has private key $XB=12$, What is *B*'s public key *YB*

(iii) What is the ciphertext of $M=30$? (16)

14. (a) Explain the denial of service attacks. What kinds of damages are caused by viruses and worms. (16)

Or

(b) What is IDS? Explain in detail about various intrusion detection systems. (16)

15. (a) Explain the use of cryptographic and network security techniques for an online shopping application. (16)

Or

(b) (i) Illustrate the need for using firewalls to provide system security. (8)

(ii) What are the various security factors you need to consider when you develop a banking application? (8)