[Total No. of Questions - 8] [Total No. of Printed Pages - 2]
(2124)

1661

M. Tech 3rd Semester Examination

Information Security

EC-305

Time : 3 Hours **Max. Marks : 100**

The candidates shall limit their answers precisely within the answer-book (40 pages) issued to them and no supplementary/continuation sheet will be issued.

Note : Attempt any five questions.

1. (a) Prove or disprove double DES is better than single DES.

   (b) Describe Fiestal function used in DES.

   (c) What are the different types of active attacks? Explain each briefly. (4+6+10=20)

2. (a) Explain key generation for encryption and decryption in IDEA. Also give encryption technique.

   (b) What are the different types of attacks that can be performed on encrypted plaintext? (8+8+4=20)

3. (a) What do you mean by public key cryptosystem? Explain RSA algorithm.

   (b) If n and ϕ (n) are known to an attacker, how can RSA be attacked?

   (c) Define message authentication code and cryptographic hash function. (2+6+6+6=20)

[P.T.O.]

4. (a) Define elliptic curve in Z_n. Explain the addition and multiplication operations in this elliptic curve system.

   (b) Explain encryption and decryption in ECC.

   (c) Write Diffie-Hellman key exchange algorithm. How can it be attacked? (8+6+4+2=20)

5. (a) Explain the structure of HMAC. On what factors is the security HMAC based on?

   (b) Describe the Kerberose mechanism for mutual authentication. (10×2=20)

6. (a) Explain PGP technique for confidentiality only, authentication only and confidentiality & authentication for e-mail.

   (b) Explain the file system security in LINUX. (12+8=20)

7. (a) Describe briefly SSL protocol stack.

   (b) What are the three functional areas which IPsec encompasses? Also describe IPsec document categorization. (10×2=20)

8. Write short notes on any two:

   (a) Triple DES OFB.

   (b) Intrusion detection techniques.

   (c) Side channel attacks.

   (d) X.319 Directory Authentication scheme. (10×2=20)