2016/ODD/12/32/IT–703/627

B.Tech Odd Semester (CBCS) Exam.,
December—2016

INFORMATION TECHNOLOGY

(7th Semester)

Course No. : IT–703

(Cryptography and Network Security)

Full Marks : 75
Pass Marks : 30

Time : 3 hours

The figures in the margin indicate full marks for the questions

Answer **five** questions, taking **one** from each Unit

UNIT—1

1. *(a)* What is the OSI security architecture? List and briefly define the categories of security mechanisms. 1+4=5

(b) Explain the message encryption and decryption processes using one time pad (OTP). What are two practical problems in its use? 4+2=6

(c) Using the extended Euclidean algorithm, find the multiplicative inverse of 24140 mod 40902. 4

2. *(a)* Draw a matrix to show the relationship between security services and attacks as defined in OSI security architecture. 4

(b) Distinguish between a monoalphabetic cipher and a polyalphabetic cipher. Explain the playfair cipher with an example. 2+4=6

(c) Determine the gcd of the following pairs of polynomials : 5

$$x^3 \quad x \quad 1 \text{ and } x^2 \quad x \quad 1 \text{ over GF(2)}$$

UNIT—2

3. *(a)* Briefly explain triple DES with two keys. 5

(b) State the strengths and weaknesses of DES. Explain the avalanche effect in DES. 3+3=6

(c) Which parameters and design choices determine the actual algorithm of a Feistel cipher? 4

4. *(a)* Explain the key generation process of data encryption standard (DES) algorithm. Explain the functioning of S-boxes in DES with an example. What is the purpose of the S-boxes in DES? 4+3+2=9

(b) Explain cipher block chaining (CBC) and cipher feedback (CFB) modes of block cipher operation. Also mention their advantages and limitations. 6

UNIT—3

5. *(a)* Describe a qualitative pseudorandom sequence generator. 5

(b) How does KDC allow Bob. Alice to determine shared symmetric secret key to communicate with each other? Explain. 4

(c) Describe the AES key expansion algorithm. 6

6. *(a)* Explain IDEA in detail. Mention the application areas of IDEA. 7+2=9

(b) How is AES decryption process different from encryption? Explain. 6

UNIT—4

7. *(a)* Explain the Elgamal public key cryptosystem. 8

(b) Describe SHA-1 algorithm and compare its features with MD5. 5+2=7

8. *(a)* Explain the Diffie-Hellman key exchange algorithm with an example. 5

(b) Perform encryption and decryption for p 7, q 11, e 13 and m 2 using RSA. 5

(c) Write the Rabin-Miller primality testing algorithm. Test the primality of the number 221 using this algorithm. 3+2=5

UNIT—5

9. *(a)* What are the properties of digital signature? Explain the DSA key generation, signature creation and signature verification process. 3+6=9

(b) Explain the format of X.509 certificate. 6

10. *(a)* Give an overview of elliptic curve cryptosystem. 8

(b) What is the use of Kerberos? Explain the Kerberos v5. 2+5=7

★ ★ ★