CBCS SCHEME

USN | | | | | | | | | | |

15TE71

Seventh Semester B.E. Degree Examination, Dec.2018/Jan.2019
Cryptography and Network Security

Time: 3 hrs. Max. Marks: 80

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

1 a. Define the term cryptography. Explain the essential components of conventional encryption. **(06 Marks)**

b. Find GCD (1970, 1066) using extended Euclidean algorithm. **(04 Marks)**

c. List the rules applied for encryption of plain text message using play fair cipher. Obtain the cipher text for the message "WE WILL MEET TOMORROW" using key "STORY". **(06 Marks)**

OR

2 a. Prove the following property of modular arithmetic and hence verify with a = 11, b = 15 and n = 8. [(a mod n) – (b mod n)]mod n = (a – b) mod n **(06 Marks)**

b. Encrypt the plain text "MONDAY" using Hill cipher with key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Show your calculations in obtaining cipher text. [Use a = 0, b = 1, …. Z = 25] **(06 Marks)**

c. Explain transposition cipher with an example. **(04 Marks)**

Module-2

3 a. What are the differences between Block cipher and stream cipher? **(04 Marks)**

b. Explain the parameters on which design of Feistel network depends on. **(06 Marks)**

c. In RSA scheme it is given that two prime numbers p = 7 and q = 11. The plain text message M = 8. Find the cipher text. **(06 Marks)**

OR

4 a. What are the requirements that public key crypto system must fulfill to become more secure algorithm? **(06 Marks)**

b. User A and user B use Diffie-Hellman key exchange technique with common prime q = 71, and a primitive root $\alpha = 7$. Find:
i) A's public key K_A, if A has private key $X_A = 5$
ii) B's public key K_B, if B has private key $X_B = 12$
iii) Shared secrete key K_{AB}. **(06 Marks)**

c. Explain steps involved in encryption and decryption of a message using RSA algorithm. **(04 Marks)**

Module-3

5 a. Explain basic steps involved in generation of hash code using MD5 algorithm. **(10 Marks)**

b. What are the design goals of MD4? Explain them. **(06 Marks)**

OR

6 a. What are the requirements should a digital signature scheme must satisfy? **(06 Marks)**

b. Bring out the differences between MD5 and SHA. **(05 Marks)**

c. What is Message Authentication Code (MAC)? Explain MAC generation and verification in CBC-MAC. **(05 Marks)**

Module-4

7 a. Explain the steps involved in operation of SSL record protocol with a neat diagram. **(10 Marks)**

b. List and briefly explain the parameters that define an SSL session state. **(06 Marks)**

OR

8 a. What are the security services addressed by IEEE 802.11i? **(06 Marks)**

b. With a neat diagram briefly describe the four IEEE 802.11i phases of operation. **(10 Marks)**

Module-5

9 a. What are the five principal services provided by PGP? **(05 Marks)**

b. Explain the digital signature service provided by PGP with a neat diagram. **(05 Marks)**

c. List and explain various functionalities of S/MIME. **(06 Marks)**

OR

10 a. Write a neat diagram showing an architecture of IPSec. Explain various parameters in Security Association Database (SAD) entry. **(10 Marks)**

b. What are the three uniquely identified Security Association Parameters in IPSec? Explain them. **(06 Marks)**

* * * * *