CBCS SCHEME

USN □□□□□□□□□□

15TE71

## Seventh Semester B.E. Degree Examination, Dec.2019/Jan.2020

# Cryptography and Network Security

Time: 3 hrs. Max. Marks: 80

**Note:** ***Answer FIVE full questions, choosing one full question from each module.***

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

## Module-1

1 a. Describe the additive and multiplicative inverse modulo 8 in finite fields of the form GF($2^n$). **(06 Marks)**

b. Explain transposition Ciphers with an example. **(04 Marks)**

c. Outline the concept of groups, rings and fields. **(06 Marks)**

**OR**

2 a. Explain the Euclidean algorithm with an example. **(05 Marks)**

b. Describe one time pad encryption technique with an example and its difficulties. **(05 Marks)**

c. Briefly explain the Caeser, Playfair and Hill Ciphers, with example. **(06 Marks)**

## Module-2

3 a. Illustrate the Feistel Encryption and Decryption process with its structure. **(06 Marks)**

b. With relevant diagram, explain the process of AES Encryption. **(06 Marks)**

c. Explain RSA algorithm. **(04 Marks)**

**OR**

4 a. Illustrate the process of DES encryption with diagram. **(06 Marks)**

b. Explain Diffie - Hellman key exchange algorithm. **(04 Marks)**

c. With the help of neat diagram, explain elliptic curve arithmetic and rules. **(06 Marks)**

## Module-3

5 a. Explain surface and about its cryptanalysis. **(05 Marks)**

b. Outline N-Hash algorithm with neat diagram. **(06 Marks)**

c. Discuss the design goals of MD4 Algorithm. **(05 Marks)**

**OR**

6 a. Explain MD5 Hash function. **(05 Marks)**

b. Describe Secure Hash Function with one SHA operation **(06 Marks)**

c. Explain DSA algorithm. **(05 Marks)**

## Module-4

7 a. With the help of block diagram, explain SSH protocol stack. **(04 Marks)**

b. Draw the neat flow diagram and explain Hand Shake protocol Action in SSL. **(06 Marks)**

c. Explain IEEE 802.11i phases of operation with flow diagram. **(06 Marks)**

**OR**

8 a. Explain SSL protocol stack with session state and connection status parameters. **(05 Marks)**

b. With neat flow diagram, explain SSH transport layer protocol packets exchanger and packet formation. **(07 Marks)**

c. Explain IEEE 802.11i services and protocols. **(04 Marks)**

## Module-5

9 a. Explain PGP cryptographic functions with relevant diagram. (10 Marks)

b. With the help of diagram, explain typical scenario of IP security usage. (06 Marks)

**OR**

10 a. Describe the cryptographic algorithms used in S/MIME. (07 Marks)

b. Identify the fields in top level ESP packet format. (05 Marks)

c. Briefly explain the applications of IP security. (04 Marks)

* * * * *