CBCS SCHEME

USN □□□□□□□□□□

18ECS243

Second Semester M.Tech. Degree Examination, June/July 2019

Cryptography and Network Security

Time: 3 hrs. Max. Marks: 100

Note: Answer any 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. Explain four types of substitution ciphers. **(10 Marks)**

b. Explain with neat block diagram encryption and decryption and explain authentication, integrity and non-repudiation. **(10 Marks)**

OR

2 a. Explain with diagram general depiction of DES encryption algorithm. **(10 Marks)**

b. Explain with diagram of AES key expansion. **(10 Marks)**

Module-2

3 a. State and prove Fermat's theorem and Euler's theorem. **(10 Marks)**

b. Explain first assertion and second assertion of the Chinese remainder theorem. **(10 Marks)**

OR

4 a. Describe RSA algorithm and discuss the security of RSA. **(10 Marks)**

b. Explain Diffie-Hellman key exchange algorithm. **(10 Marks)**

Module-3

5 a. Explain linear complexity and correlation immunity. **(10 Marks)**

b. Explain with diagram of Jennings generator. **(10 Marks)**

OR

6 a. Explain: i) Fish ii) Dike iii) Mush. **(10 Marks)**

b. Explain with diagram GIFFORD. **(10 Marks)**

Module-4

7 a. Explain with diagram of MD5 main loop. **(10 Marks)**

b. Explain with diagram of the four secure hash functions where the block length equals the hash size. **(10 Marks)**

OR

8 a. Explain: i) RIPE-MAC ii) IBC-Hash. **(10 Marks)**

b. Explain GOST digital signature algorithm and its parameters. **(10 Marks)**

Module-5

9 a. Explain Pretty Good Privacy. **(10 Marks)**

b. Explain the five header fields defined in MIME. **(10 Marks)**

OR

10 a. List the top-level format of an ESP packet. **(10 Marks)**

b. Explain SSL record protocol operation. **(10 Marks)**

* * * * *