CBCS SCHEME

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

20ECS243

Second Semester M.Tech. Degree Examination, July/August 2022
Cryptography and Networks Security

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Briefly describe about steganography. **(04 Marks)**
b. With a neat diagram,, explain DES encryption algorithm. **(08 Marks)**
c. Explain how the S-Box is constructed in AES algorithm. **(08 Marks)**

OR

2 a. Write short notes on One-Time pad. **(04 Marks)**
b. With a neat diagram, explain the Feistel encryption and decryption algorithm. **(08 Marks)**
c. With a neat diagram, explain the AES encryption and decryption process. **(08 Marks)**

Module-2

3 a. State and prove Fermat's and Euler's theorem. **(10 Marks)**
b. Explain ECC Diffie-Hellman key exchange algorithm. **(10 Marks)**

OR

4 a. Explain the RSA algorithm. In a RSA algorithm system it is given that p = 17, q = 11, e = 7 and M = 88. Find the cipher text 'e' and encrypt 'C' to set plain text M. **(10 Marks)**
b. With an example, explain logarithms for modular arithmetic and state the properties of logarithms. **(10 Marks)**

Module-3

5 a. With a neat diagram, explain linear feedback shift registers. **(06 Marks)**
b. Explain :
i) Linear complexity
ii) Correlation immunity. **(06 Marks)**
c. With a neat diagram, explain the construction and generation of self decimated generators and Gollmann cascade. **(08 Marks)**

OR

6 a. Write short notes on linear congruential generator. **(06 Marks)**
b. Explain :
i) Geff Generator
ii) Beth – pipes and go-generator. **(06 Marks)**
c. Explain the encryption algorithm that is designed to build PKZIP data compression program. **(08 Marks)**

Module-4

7 a. Explain one way Hash function. Explain how Alice uses the birthday attack to swindle Bob. **(08 Marks)**
b. Explain Message Authentication Algorithm (MAA). **(04 Marks)**
c. Describe the steps involved in the NIST recommended specific method for generating two primes p and q where, q divides p – 1. **(08 Marks)**

OR

8 a. Explain N-Hash algorithm and cryptanalysis of N-Hash. (10 Marks)

b. List the Rivest's MD5 improvements to MD4, and how are they compared with SHAs. (06 Marks)

c. List the four criticism against digital signature algorithm. (04 Marks)

Module-5

9 a. What are the confidentiality and authentication services provided by PGP and explain the five reasons for the growth of PGP. (10 Marks)

b. With neat diagram of DKIM functional flow, explain each elements of the DKIM operation. (10 Marks)

OR

10 a. With a neat diagram, explain PGP cryptographic function. (10 Marks)

b. Describe the threats addressed by DKIM interms of the characteristics, capabilities and location of potential attaches. (10 Marks)

* * * * *