CBCS SCHEME

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

20ECS243

Second Semester M.Tech. Degree Examination, Jan./Feb. 2023
Cryptography and Network Security

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Explain four general types of cryptanalytic attacks. **(08 Marks)**

b. What is substitution cipher, list different types of substitution cipher and also explain Caesar Cipher with example. **(08 Marks)**

c. Describe the operation of rotor machine technique with example. **(04 Marks)**

OR

2 a. With the help of neat diagram, explain over all scheme for DES encryption. **(10 Marks)**

b. Explain AES encryption process in detail. **(10 Marks)**

Module-2

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

b. Write note on Chinese reminder theory and explain discrete logarithms. **(10 Marks)**

OR

4 a. With necessary diagram explain public key crypto system. Also summarize some important aspects of symmetric and public key encryption with authentication and secrecy. **(10 Marks)**

b. Explain RSA algorithm with example. **(10 Marks)**

Module-3

5 a. List some advantages and disadvantages of linear congruential generators. **(04 Marks)**

b. Describe the operation of 4 bit LFSR with example. **(08 Marks)**

c. Write note on linear complexity and correlation immunity with respect to stream cipher. **(08 Marks)**

OR

6 a. Describe the operation of generalized Geffe generator and Beth piper stop and go generator. **(10 Marks)**

b. Write note on Gifford encryption technique used in stream cipher and PKZIP data compression program. **(10 Marks)**

Module-4

7 a. Explain out line of N Hash. **(10 Marks)**

b. Explain MD4 and MD5 one way Hash function. **(10 Marks)**

OR

8 a. Describe Importance of SHA in DSA. **(10 Marks)**

b. Explain key depended one way Hash function. **(10 Marks)**

Module-5

9 a. List out services provided by "PGP" and show how confidentiality and authentication is obtained. **(10 Marks)**

b. Explain what are the functionality provided by "S/MIME". **(10 Marks)**

OR

10 a. Elaborate an overview of IP security scenario and also explain IP security architecture. **(10 Marks)**

b. Explain SSL with respect to Web Security. **(10 Marks)**

* * * * *