CBCS SCHEME

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

15TE71

Seventh Semester B.E. Degree Examination, Jan./Feb. 2021
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. Explain the Euclidean algorithm. **(08 Marks)**

b. Explain the Fermat's and Euler's theorem. **(08 Marks)**

OR

2 a. What is Cryptanalysis? Explain any three general types of cryptanalysis attacks. **(08 Marks)**

b. Explain the substitution ciphers and transposition ciphers. **(08 Marks)**

Module-2

3 a. Explain with neat diagram general depiction of DES encryption algorithm. **(06 Marks)**

b. With a block diagram, explain AES encryption and decryption algorithm. **(10 Marks)**

OR

4 a. Explain the RSA algorithm in detail. **(08 Marks)**

b. Explain elaborately Diffie-Hellman key exchange. **(08 Marks)**

Module-3

5 a. With a schematic, explain the outline and one processing stage of N-Hash function. **(08 Marks)**

b. With a schematic, explain secure hash algorithm in detail. **(08 Marks)**

OR

6 a. Explain the digital signature algorithm. Also explain the singing and verifying function of digital signature algorithm. **(10 Marks)**

b. Explain the discrete logarithm signature schemes. **(06 Marks)**

Module-4

7 a. Elucidate TLS Architecture. **(08 Marks)**

b. Discuss HTTPs. **(08 Marks)**

OR

8 a. Explain the SSH protocol stack. **(08 Marks)**

b. Explain the IEEE 802.11i phases of operation. **(08 Marks)**

Module-5

9 a. Explain the pretty good privacy protocol. **(06 Marks)**

b. With a neat diagram, explain the simplified S/MIME functional flow. **(10 Marks)**

OR

10 a. Explain the benefits of IP security. **(06 Marks)**

b. Explain IP security architecture. **(10 Marks)**

* * * * *