Code No: **R1641051** **R16** **Set No. 1**

IV B.Tech I Semester Supplementary Examinations, July/Aug - 2021

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any FOUR questions from Part-B

*****

PART–A *(14 Marks)*

1. a) Explain the terms Authenticity and Accountability. [2]
   b) Explain the need for encryption. [3]
   c) What is a primitive root of a number? Give example. [2]
   d) What is message authentication? [2]
   e) List and briefly define the parameters that define an SSL session connection. [2]
   f) What services are provided by IPsec? [3]

PART–B *(4x14 = 56 Marks)*

2. a) With a neat diagram explain the Model for Network Security. [7]
   b) Explain the Challenges of Computer Security. [7]

3. a) Explain about the DES with a suitable example. [7]
   b) Present an overview of the general structure of Advanced Encryption Standard. [7]

4. a) Discuss key concepts relating to prime numbers. [7]
   b) Explain about Diffie Hellman Key Exchange. [7]

5. a) Explain the basic structure of cryptographic hash functions. [7]
   b) Present an overview of approaches to public-key distribution and analyze the risks involved in various approaches. [7]

6. a) Explain about MIME (Multipurpose Internet Mail Extension). [7]
   b) What protocols comprise SSL? What is the difference between an SSL connection and an SSL session? Briefly define the parameters that define an SSL session state. [7]

7. a) Summarize the traffic processing functions performed by IPsec for outbound packets and for inbound packets. [7]
   b) Explain the distinctions between Host-based and Network-based IDS/IPS. [7]