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

IV B.Tech I Semester Supplementary Examinations, February - 2020

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and 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 four main groups of Cryptographic algorithms and protocols. [2]
   b) Explain the encryption and decryption. [2]
   c) What is the difference between an index and a discrete logarithm? [2]
   d) What are some threats associated with a direct digital signature scheme? [2]
   e) Why does PGP generate a signature before applying compression? Explain. [3]
   f) Explain the difference between transport mode and tunnel mode. [3]

PART–B *(4x14 = 56 Marks)*

2. a) Discuss the types of security threats and attacks that must be dealt with and give examples of the types of threats and attacks that apply to different categories of computer and network assets. [7]
   b) Explain about Caesar Cipher and Mono alphabetic Ciphers [7]

3. a) It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible?. [7]
   b) Explain the four transformations used in AES. [7]

4. a) Present an overview of the basic principles of public-key cryptosystems. [7]
   b) Present an overview of the RSA algorithm. [7]

5. a) Explain about the Digital Signature process. [7]
   b) Explain about the Key Management. [7]

6. a) List the parameters that define an SSL session state and explain the services provided by the SSL record protocol. [7]
   b) Explain the five principle services provided by PGP (Pretty Good Privacy). [7]

7. a) What are IPsec functional areas? Explain the IPsec key management.. [7]
   b) Discuss the alternatives for combining security associations. [7]

||''|''|''|''||