RT41051102019 - Cryptography and Network Security exam paper for BTech

B.Tech (Uttarakhand Technical University)

Code No: **RT41051** **R13** **Set No. 1**

IV B.Tech I Semester Supplementary Examinations, October/November - 2019

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 THREE questions from Part-B
*****

PART–A *(22 Marks)*

1. a) What is the web based attacks? [3]
   b) What are the disadvantages of double DES? [4]
   c) State Euler's Theorems. [3]
   d) What is meant by one-way property in hash function? [4]
   e) What is the problem that kerberos addresses? [4]
   f) What is meant by intrusion detection system? [4]

PART–B *(3x16 = 48 Marks)*

2. a) Differentiate between passive attacks and active attacks. [8]
   b) Discuss about TCP session hijacking and UDP hijacking. [8]

3. a) Describe Triple DES and its applications. [8]
   b) Discuss in detail about Blowfish. [8]

4. a) Describe RSA Algorithm and Estimate the encryption and decryption values for the RSA algorithm parameters. [8]
   b) State the Chinese Remainder Theorem and find X for the given set of congruent equations $X \equiv 2 \bmod 3$, $X \equiv 3 \bmod 5$ and $X \equiv 2 \bmod 7$. [8]

5. a) What are the types of attacks addressed by message authentication? What are two levels of functionality that comprise a message authentication or digital signature mechanism? [8]
   b) Explain the process of deriving eighty 64-bitwords from 1024 bits for processing of a single blocks and also discuss single round function in SHA-512 algorithm. Show the values of W16, W17, W18 and W19. [8]

6. a) How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components. [8]
   b) Analyze the Cryptographic algorithms used in S/MIME and Explain S/MIME certification processing. [8]

7. a) Explain IP Security protocols in detail. [8]
   b) Write short notes on Signature based IDS. [8]