

RA

Code No: 137SH

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech IV Year I Semester Examinations, October/November - 2020

CRYPTOGRAPHY AND NETWORK SECURITY

(Information Technology)

Time: 2 hours

Max. Marks: 75

Answer any Five Questions
All Questions Carry Equal Marks

- 1.a) How security services are related to security mechanisms?
- b) List and explain the possible types of attacks. [8+7]
2. Explain the substitution techniques and transposition techniques with examples. [15]
3. Explain the principles of Public key cryptosystems. Discuss the Knapsack algorithm.[15]
4. Write down the code snippet for AES algorithm and explain with a neat diagram. [15]
5. Explain how SHA-512 algorithm works. [15]
6. List and explain the techniques used for public key distribution. Also, explain how session key is exchange using public key cryptography. [15]
7. How SSL Handshake protocol establishes a session? Explain in detail. [15]
- 8.a) Discuss the significance of each field of Public key ring data structure in PGP.
- b) With the help of neat diagram, explain the IP security architecture. [8+7]

---ooOoo---