Code No: 138DT **R16**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year II Semester Examinations, September - 2020
NETWORK SECURITY AND CRYPTOGRAPHY
(Electronics and Communication Engineering)

Time: 2 Hours **Max. Marks: 75**

Answer any Five Questions
All Questions Carry Equal Marks
- - -

1.a) Explain with a neat diagram the Model of Symmetric Cryptosystem.
b) Write a detailed note on Monoalphabetic Ciphers. [8+7]

2. Describe the RC5 method used for encryption and decryption. [15]

3. Write a detailed note on International Data Encryption algorithm. [15]

4. Briefly describe the idea behind Elliptic Curve Cryptosystem and describe the key management of public key. [15]

5.a) Use Fermat's theorem to find a number a between 0 and 72 with a congruent to 9794 modulo 73.
b) Use Euler's theorem to find a number x between 0 and 28 with x^{85} congruent to 6 modulo 35. [7+8]

6. Explain in detail about Digital Signatures. Show how signing and verification is done using Digital Signature Standards. [15]

7. Compare and generalize the features of SHA and MD5 algorithm. [15]

8.a) Explain with a neat diagram the SSL Record Protocol.
b) Write down the applications of IPsec. [8+7]

---ooOoo---

JNTUH USED PAPER Sep-2020