

R19

Code No: 863AE

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD**MCA III Semester Examinations, February - 2021****INFORMATION SECURITY****Time: 2 hours****Max. Marks: 75**

Answer any five questions
All questions carry equal marks

- - -

- 1.a) What is a Transposition Cipher?
- b) What is Steganography? [8+7]
- 2.a) What is the purpose of the S-boxes in DES?
- b) What is the difference between Differential and Linear Cryptanalysis? [7+8]
3. Write a detailed note on the RSA Algorithm. List out the Four possible approaches to attack the RSA algorithm. [15]
4. Write a detailed note on SHA-512 Algorithm. [15]
5. Explain in detail the Digital Signature Algorithm. [15]
6. Explain with a neat diagram various PGP Cryptographic Functions. [15]
7. Explain with a neat diagram the ESP (Encapsulating Security Payload) Packet Format. [15]
8. What is a Firewall? Explain various types of Firewalls with neat diagrams. [15]

---oo0oo---