

AG AG AG AG AG AG AG A

**R16**

Code No: 136AW

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech III Year II Semester Examinations, November/December - 2020

**CRYPTOGRAPHY AND NETWORK SECURITY**

(Common to CSE, IT)

AG AG AG AG AG AG AG A

Time: 2 hours

Max. Marks: 75

Answer any five questions  
All questions carry equal marks

---

AG AG AG AG AG AG AG A

- 1.a) Differentiate between Symmetric and Asymmetric cryptographic techniques.  
b) Write about Integrity and Non-repudiation Security Services. [8+7]

2. Enumerate in detail the steps in Data Encryption Standard Algorithm and explain the process involved in each round with a neat diagram. [15]

AG AG AG AG AG AG AG A

3. What is the purpose of SHA-1 Algorithm? What is the length of message digest and key size in SHA-1 Algorithm? Discuss about all the rounds in SHA-1 algorithm. [15]

AG AG AG AG AG AG AG A

- 4.a) Write about the functionalities of Transport Layer Security Protocol.  
b) Describe the security constraints of HTTP protocol. [7+8]

5. Write short note on:  
a) S/MIME  
b) Authentication Header Protocol. [8+7]

AG AG AG AG AG AG AG A

- 6.a) Write any three substitution ciphers with examples.  
b) Describe man-in-the-middle attack and compare with ARP attack. [7+8]

- 7.a) Explain all the parameters in Feistel Block Cipher Structure.  
b) Describe the encryption process in IDEA algorithm with a neat sketch. [6+9]

AG AG AG AG AG AG AG A

- 8.a) What is Digital Signature? Describe the procedure how to get Digital Certificates.  
b) Write about X.509 Directory Authentication Service. [7+8]

---ooOoo---

AG AG AG AG AG AG AG A

AG AG AG AG AG AG AG A