Code No: 137SH **RA**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, December - 2019
CRYPTOGRAPHY AND NETWORK SECURITY
(Information Technology)

Time: 3 Hours **Max. Marks: 75**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b as sub questions.

PART – A

(25 Marks)

1.a)	Write any two differences of Transposition and Substitution Ciphers.	[2]
b)	Describe briefly about Denial-of-service.	[3]
c)	List the principles of public key cryptography.	[2]
d)	What are the weaknesses of DES?	[3]
e)	Write short notes on Kerberos.	[2]
f)	Define Message Authentication code.	[3]
g)	Define Transport Layer Security.	[2]
h)	Draw SSL Protocol Stack.	[3]
i)	Define MIME.	[2]
j)	List the services provided by PGP.	[3]

PART – B

(50 Marks)

2. Discuss the operations, requirements, components of Network security model. [10]

OR

3. Discuss the relation between security mechanisms and attacks. [10]

4. Illustrate Block Cipher Modes of operation with relevant diagrams. [10]

OR

5. Explain RSA encryption and decryption algorithms. Given two prime numbers p=5 and q=11, and encryption key e=7. Derive the decryption key d. Let the message be M=10. Perform the encryption and decryption using RSA algorithm. [10]

6. Define Digital Signature. Explain the approaches for Digital Signatures based on Public Key Encryption. [10]

OR

7. Client machine C wants to communicate with server S. Explainhow the communication can be achieved through Kerberos protocol? [10]

8. Describe the SSL Specific protocol – Handshake action in detail. [10]

OR

9. Explain about various security issues in Transport Layer. [10]

10.a) How the messages are generated and transmitted in pretty good privacy (PGP) protocol? Explain with clear diagrams.

b) Explain the steps involved in performing Secure Inter-branch Payment Transactions.[4+6]

OR

11.a) Give IP Security architecture with neat diagram.

b) Discuss in detail Encapsulating Security Payload (ESP). [4+6]

---ooOoo---