JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, December - 2019
CRYPTOGRAPHY AND NETWORK SECURITY
(Common to CSE, IT)

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, c as sub questions.

PART - A
(25 Marks)

1.a)	Differentiate between Interruption and Interception.	[2]
b)	Discuss about Masquerade in brief.	[3]
c)	List out the advantages of RC4 algorithm.	[2]
d)	Write about cipher block chaining mode of operation.	[3]
e)	What is the key size and Message Digest size in SHA1 algorithm?	[2]
f)	What are the benefits of Digital Signature?	[3]
g)	Summarize the functions of HTTP protocol.	[2]
h)	Discuss about the importance of security in mobile devices.	[3]
i)	What are the applications of IPSec?	[2]
j)	What are the advantages of Authentication Header Protocol?	[3]

PART - B
(50 Marks)

2.a)   Describe the model for network security with neat sketch.
  b)   Describe pervasive and specific security mechanisms in detail.   [4+6]

OR

3.a)   Write any three transposition ciphers with examples.
  b)   Discuss about Brute force attack in detail.   [6+4]

4.a)   Summarize the public key cryptographic principles. Explain RSA algorithm for given example, where p = 3 and q = 11.
  b)   Enumerate Diffie-Hellman Key exchange for encryption and decryption with suitable examples.   [5+5]

OR

5.   Enumerate in detail about the steps in Blow Fish Algorithm and explain the process of each round with a neat diagram.   [10]

6.a)   What is HMAC function? Summarize the design objectives of HMAC.
  b)   Explain about Elgamal Digital Signature Scheme.   [5+5]

OR

7.   Discuss about the message exchange mechanism in Kerberos version 4.   [10]

8.a) What is SSL? Explain about SSL record protocol format.
  b) Enumerate the functionalities of Secure Shell.   [6+4]

OR

9. Explain the security constraints of IEEE 802.11i Wireless LAN in detail.   [10]

10. Write general format of PGP message with a pictorial representation and explain. How PGP used for E-mail security?   [10]

OR

11.a) Describe the functionalities of Internet Key Exchange Protocol.
   b) How to provide security during Inter-branch Payment Transactions?   [5+5]

---ooOoo---