Code No: 136AW

R16

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, May - 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)	What are security mechanisms? Explain.	[2]
b)	What is steganography?	[3]
c)	Do you agree with the statement that an increase in key size of 1 bit doubles the security of DES? Justify your answer.	[2]
d)	How keys are exchanged in Diffie-Hellman algorithm?	[3]
e)	Give a note on public key infrastructure.	[2]
f)	What problem was Kerberos designed to address? Explain.	[3]
g)	In SSL and TLS, why is there a separate change cipher spec protocol, rather than including change cipher spec message in the handshake protocol?	[2]
h)	Explain the IEEE 802.11Wireless LAN.	[3]
i)	What is transport mode and tunnel mode in IP sec?	[2]
j)	Give a brief note on Virtual Elections.	[3]

PART - B

(50 Marks)

2.a) List and briefly define categories of Security Services and attacks.
b) How would you test a piece of cipher text to determine quickly if it was likely the result of a simple substation? Explain. [5+5]

OR

3. Consider a desktop publishing system used to produce documents for various organizations.
a) Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.
b) Give an example of a type of publication in which data integrity is the most important requirement.
c) Give an example in which system availability is the most important requirement.[10]

4. AES consists of four functions in three layers. Which of the functions are primarily for confusion and which are primarily for diffusion? Which of the layers are for confusion and which are for diffusion? Justify your answers. [10]

OR

5.a) Critically analyze the security of RSA.
b) Differentiate between RC_5 and blowfish. [5+5]

6. List the main features of SHA-512 cryptographic hash function. What kind of compression function is used in SHA-512? [10]

OR

7. Explain Message Authentication Requirements and what are the attacks related to message communication? [10]

8. Is it possible in SSL for the receiver to recorder SSL record blocks that arrive out of order? If so, explain how it can be done. If not, why not? [10]

OR

9. Discuss the IEEE 802.11i Wireless LAN Security. [10]

10.a) Briefly explain the scenario of IP security and its Policy.
b) Explain IP security architecture and also explain basic combinations of security associations with a neat diagram. [5+5]

OR

11. List and explain the PGP services and explain how PGP message generation is done with a neat diagram. [10]

---oo0oo---