Code No: 157BB **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, December-2023/January-2024
CRYPTOGRAPHY AND NETWORK SECURITY
(Common to CSE, CSE(N))

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

Note: i) Question paper consists of Part A, Part B.
ii) Part A is compulsory, which carries 25 marks. In Part A, answer all questions.
iii) In Part B, Answer any one question from each unit. Each question carries 10 marks and may have a, b as sub questions.

PART - A

(25 Marks)

1.a)	List the various types of Security Attacks.	[2]
b)	Explain the need for security.	[3]
c)	Do you agree with the statement that an increase in the key size of 1 bit doubles the security of DES? Justify your answer.	[2]
d)	What primitives operations are used in RC4? Explain.	[3]
e)	What are Digital Signatures?	[2]
f)	What are the attacks related to message communication?	[3]
g)	Draw the SSL Message Formats.	[2]
h)	Discuss the IEEE 802.11 Wireless LAN.	[3]
i)	What is IP security and its benefits?	[2]
j)	List the types of PGP.	[3]

PART – B

(50 Marks)

2.a) Discuss about security approaches.
b) How security services are related to security mechanisms? Explain. [5+5]

OR

3.a) Explain Hill cipher with an example.
b) Compare and contrast the substitution techniques and transposition techniques. [5+5]

4. Explain Diffie- Hellman key exchange protocol in detail. Consider a Diffie- Hellman key with a common prime q=11 and primitive root $\alpha = 2$ If the user has a public key $Y_a = 9$, then what is A's private key X_A? [10]

OR

5.a) Write the differences among DES, AES, Blowfish, IDEA and RC5 in terms of the Number of rounds, block size, key size.
b) Give a brief note on Block Ciphers and Stream Ciphers. [6+4]

6. Give a detailed note on how hash value is produced for an arbitrary size message in SHA-512. [10]

OR

7. Discuss the Elgamal Digital Signature Scheme in detail. [10]

8. Explain the SSL Handshake protocol with relevant illustrations in detail. [10]

OR

9.a) Explain the HTTP, and Secure Shell (SSH).
b) Discuss about Mobile Device Security. [5+5]

10.a) With the help of a neat diagram, explain the IP security architecture.
b) In PGP, can an e-mail message use two different public key algorithms for encryption and signing? How is this defined in a message sent from Alice to Bob? [5+5]

OR

11. What is the purpose of MIME and S/MIME? List and explain the types of messages in S/MIME and their purposes. [10]

--oo0oo---