Code No: 157BB **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, January/February - 2023
CRYPTOGRAPHY AND NETWORK SECURITY
(Computer Science and Engineering)

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 principles of security.	[2]
b)	How security services are related to security mechanisms?	[3]
c)	Define Elgamal Cryptography.	[2]
d)	In the RSA system, the public key of a given user is e=31, n=3599 what is the private key of the user?	[3]
e)	What are the HMAC design objectives as per the RFCs?	[2]
f)	Explain Message Authentication Requirements in brief.	[3]
g)	Define Wireless Security.	[2]
h)	Discuss the Mobile Device Security.	[3]
i)	Difference between MIME and S/MIME.	[2]
j)	What is meant by cross site scripting vulnerability.	[3]

PART – B
(50 Marks)

2.a)	What is steganography? What are the similarities and differences between steganography and cryptography? What are the relative advantages and disadvantages of steganography?	
b)	Give the classification of security attacks.	[5+5]
	OR	
3.a)	A bank is performing all its financial transactions over the Internet. What kind of security is required? Illustrate with an example bank.	
b)	Draw and explain the model for Network Security.	[5+5]
4.	Explain RSA encryption. Also, critically analyze the security aspects of RSA.	[10]
	OR	
5.a)	With a neat diagram, explain one round of DES algorithm.	
b)	List and explain the Principles of public key cryptosystems.	[5+5]

6. Discuss the Symmetric Key Distribution Using Symmetric and Asymmetric Encryption. [10]

OR

7. Explain the HMAC, CMAC and Digital signatures. [10]

8. Describe the Transport Layer Security. [10]

OR

9. List the steps involved in the SSL record protocol transmission. [10]

10.a) Discuss the significance of key identifiers in a PGP Message and describe the five header fields in MIME.

b) Explain the Encapsulating security payload. [5+5]

OR

11. Discuss the implementation of security features considering Secure Inter-branch Payment Transactions case study. [10]

---oo0oo---