Code No: 156EV **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, July - 2023
CRYPTOGRAPHY AND NETWORK SECURITY
(Computer Science and Information Technology)

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)	What is the need for security?	[2]
b)	Describe the Public – Key Infrastructure.	[3]
c)	Discuss the possible types of attacks.	[2]
d)	Explain the Mobile Device Security.	[3]
e)	List the Block Cipher principles.	[2]
f)	Describe the Transport-level Security.	[3]
g)	Discuss the Blowfish algorithm.	[2]
h)	Outline the Authentication Header.	[3]
i)	Compare HMAC and CMAC.	[2]
j)	Describe E-Mail Security.	[3]

PART – B

(50 Marks)

2. Classify the substitution techniques with examples, also identify the best substitution techniques among the list. [10]

OR

3. Categorize the transposition techniques with examples, also identify the best transposition techniques among the list. [10]

4. Illustrate the AES algorithm with a use case. [10]

OR

5.a) Write the Diffie-Hellman Key Exchange algorithm.
b) Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Calculate their D-H key. [5+5]

6.a) How do you perform Symmetric Key Distribution Using Symmetric and Asymmetric Encryption.
b) How do you perform Public Key distribution? [5+5]

OR

7.a) Examine the Requirements for Authentication.
b) Identify pros and cons of X.509 Authentication Service. [5+5]

8.a) Compare and contrast Secure Socket Layer and Transport Layer Security in all aspects.
b) Examine the Web security considerations. [5+5]

OR

9.a) Examine the Wireless Security with an example.
b) How do you provide security in IEEE 802.11i Wireless LAN? [5+5]

10. Illustrate S/MIME with a use case. [10]

OR

11.a) Discuss the Virtual Elections by considering a pilot constituency Hyderabad.
b) Describe the process of Encapsulating security payload. [5+5]

---ooOoo---