R18

Code No: 156EV

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech III Year II Semester Examinations, March - 2024

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to CSIT, CSE(AI&ML), CSE(DS))

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 a cipher text?	[2]
b)	What are the key principles of security?	[3]
c)	Differentiate between block cipher and stream cipher.	[2]
d)	Do you agree with the statement that an increase in key size of 1 bit doubles the security of DES? Justify your answer?	[3]
e)	Mention the fundamental idea of HMAC.	[2]
f)	List any three hash algorithm.	[3]
g)	List out Web Security Considerations.	[2]
h)	Explain the IEEE 802.11Wireless LAN.	[3]
i)	Give a brief note on Virtual Elections.	[2]
j)	Describe the Security Combining Associations.	[3]

PART – B

(50 Marks)

2.a)	Discuss about different types of security services.	
b)	Explain about substitution technique with an example.	[5+5]
	OR	
3.a)	List and briefly define categories of security mechanisms.	
b)	Distinguish between Symmetric and Asymmetric Key Cryptography.	[5+5]
4.a)	Explain about Blowfish algorithm.	
b)	AES consists of four functions in three layers. Which of the functions are primarily for confusion and which are primarily for diffusion?	[5+5]
	OR	
5.a)	Critically analyze the security of RSA.	
b)	What are the principal elements of a public- key Cryptosystem? What are the roles of public key and private key?	[5+5]

6.a) Describe the steps in finding the message digest using SHA-512 algorithm.
b) What are the attacks related tomessage communication? [5+5]

OR

7.a) Give the structure of CMAC. What is the difference between CMAC and HMAC?
b) What is the job of key distribution center? [6+4]

8.a) Differentiate between IEEE 802.11 and 802.11i.
b) List and briefly define the parameters that define an SSL session connection, Session State. [5+5]

OR

9.a) Explain TLS in detail.
b) Explain the four protocols defined by Secure Socket Layer. [5+5]

10.a) Explain IP security architecture.
b) Explain how PGP message generation is done with a neat diagram? [5+5]

OR

11.a) Explain the general format of S/MIME.
b) Explain Internet key exchange. [5+5]

---ooOoo---