R18

Code No: 155EJ

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

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 are the essentials of cryptography?	[2]
b)	List and briefly define categories of security services.	[3]
c)	Write possible techniques for improving DES.	[2]
d)	Write down the characteristics of RC5.	[3]
e)	What is a message authentication code?	[2]
f)	In the context of Kerberos, what is secure authentication dialogue?	[3]
g)	Summarize services provided by the SSL Record Protocol?	[2]
h)	How to keep mobile users safe?	[3]
i)	List different MIME content types.	[2]
j)	Why does ESP include a padding field?	[3]

PART – B

(50 Marks)

2.a) Define Security attack. Discuss general categories of security attacks.
b) Draw and illustrate model for network security. [5+5]

OR

3.a) Distinguish between stream cipher and block cipher.
b) List and discuss substitution techniques with suitable examples. [5+5]

4.a) Elaborate parameters and features of feistel cipher structure with neat diagram.
b) Discuss implementation characteristics of Triple DES. [5+5]

OR

5.a) Discuss different types of cipher block modes of operations.
b) Perform encryption and decryption using RSA algorithm for p=3, q=11, e=7, and M=5. [5+5]

6.a) Discuss in detail about Digital Signature Standard (DSS) .
b) List and discuss different authentication procedures in X.509 certificate. [5+5]

OR

7.a) Explain the design objectives of CMAC.
b) Define Key management? Illustrate secret key distribution with confidentiality and authentication. [5+5]

8.a) Explain the components of SSL record format with neat diagram.
b) List and explain of phases of IEEE 802.11i security specification. [5+5]

OR

9.a) Compare secure socket layer and transport layer security.
b) Interpret how Secure Shell (SSH) works. [5+5]

10.a) Elaborate different encryption and authentication algorithms which are used for Authentication Header and Encapsulating Security Payload.
b) Discuss the services provided by IPSec. [5+5]

OR

11.a) Explain importance of the segmentation and reassembly functions in PGP.
b) Discuss main functionality of S/MIME. [5+5]

---ooOoo---