Code No: 156EV **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, August/September - 2024
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 are the principles of security?	[2]
b)	Explain steganography in the context of cryptography.	[3]
c)	What is Block Cipher?	[2]
d)	List four symmetric key ciphers.	[3]
e)	What is the purpose of HMAC in message authentication codes?	[2]
f)	List two examples of cryptographic hash functions, including one mentioned in the text.	[3]
g)	What is the primary purpose of Transport-level security in web applications?	[2]
h)	Name two protocols commonly used for implementing secure communication on the web.	[3]
i)	Define Secure Multiparty Calculation in the context of Case Studies on Cryptography and security.	[2]
j)	Show the steps involved in Cross-Site Scripting Vulnerability within the provided topics.	[3]

PART – B

(50 Marks)

2.a) Construct a comprehensive plan for enhancing network security in a corporate environment, utilizing a combination of security mechanism and principles.
b) Examine the motives behind different types of security attacks and categorize them based on their potential impact, providing insights into effective countermeasures. [5+5]

OR

3.a) Evaluate and justify the selection of a specific encryption technique for securing sensitive data in a given scenario, considering its strengths, weakness and overall effectiveness.
b) Propose an innovative solution to address emerging challenges in network security, combining existing concepts and introducing original elements to enhance overall resilience against evolving threats. [5+5]

4.a) How would you utilize the principles of DES and AES to construct a secure block cipher operation for a new cryptographic application?
b) Analyze and contrast the block cipher principles of Blowfish and RC5, identifying distinctive features and potential use cases. [5+5]

OR

5.a) Evaluate and justify the selection of a suitable cryptographic algorithm, considering criteria such as security, efficiency, and adaptability for a given application.

b) Propose an original stream cipher design by combining elements from existing algorithms, highlighting its potential advantages and use cases. [5+5]

6.a) Utilize the principles of Secure Hash Algorithm (SHA-512) to solve authentication challenges in a novel cybersecurity scenario.

b) Experiment with Elgamal Digital Signature Scheme to construct a secure digital authentication method for a distributed system. [5+5]

OR

7.a) Examine the motives and causes behind the choice of cryptographic hash functions in a given security protocol, analyzing the implications for message authentication.

b) Survey the functionality of Public Key Infrastructure (PKI) and take part in the inspection of its role in enhancing the security of digital communication. [5+5]

8.a) Discuss in brief about secure socket layer.

b) Explain in brief about web security. [5+5]

OR

9.a) Discuss and formulate a theory on maximizing the security of mobile devices within an IEEE 802.11i wireless LAN.

b) Create an elaborate solution for implementing Secure Shell (SSH) in a wireless network to ensure robust security measures. [5+5]

10.a) Examine the components of IP Security architecture and identify the key features of Authentication Header and Encapsulating Security Payload.

b) Evaluate the significance of Pretty Good Privacy (PGP) and S/MIME in ensuring email security, comparing their strengths and weakness in different usage scenarios. [5+5]

OR

11.a) Propose an original solution for enhancing the security of virtual elections, outlining the key elements and mechanisms to prevent tampering or manipulation.

b) Categorize the different types of security vulnerabilities associated with Cross-Site Scripting and provide a comprehensive analysis of their impact on web applications. [5+5]

---ooOoo---