Reg. No. : | | | | | | | | | | | | |

Question Paper Code:2057016

B.E. / B.Tech. DEGREE EXAMINATIONS, NOV/ DEC 2024
Seventh Semester
Information Technology
CS8792 – CRYPTOGRAPHY AND NETWORK SECURITY
(Regulation 2017)

Time: Three Hours Maximum: 100 Marks

Answer ALL questions

PART – A (10 x 2 = 20 Marks)

1. Identify two emerging security trends and their impact on modern cyber security practices.

2. Classify different types of security services and their role in safeguarding systems against attacks.

3. State the conditions for congruence of two numbers modulo n and provide an example.

4. Define a block cipher and state its key principles in symmetric encryption.

5. List the steps involved in calculating Euler's totient function $\phi(n)$for a given positive integer.

6. Define Euler's Theorem.

7. List the main components of an authentication protocol and identify how they contribute to secure communication.

8. State the main differences between a hash function and a MAC in terms of security and usage.

9. Identify two common threats to electronic mail security and list their potential impacts.

10. State the advantages of using IPsec for securing IP communications and infer its applications in VPN (Virtual Private Network) setups.

PART – B (5 x 16 = 80 Marks)

11. (a) Illustrate how security is integrated into the OSI architecture by detailing the role of each layer in providing security services and mechanisms. 16

(OR)

(b) Explain the process of cryptanalysis and its impact on the development of secure cryptosystems. 16

12. (a) Identify the properties of finite fields and explain their role in symmetric key cryptography. 16

(OR)

(b) Illustrate the methods used to ensure secure key distribution in cryptographic systems, highlighting the challenges and solutions for maintaining confidentiality and integrity during the key exchange process. 16

13. (a) Explain the roles of Euler's Totient Function and Euler's Theorem in RSA key generation, how Fermat's Theorem aids in simplifying modular arithmetic to enhances the computational efficiency of cryptographic operations. 16

(OR)

(b) Analyze the implementation of RSA and elliptic curve cryptography (ECC) in secure communications by selecting a specific application, such as SSL/TLS or a secure messaging platform. Discuss the strengths and weaknesses of each cryptographic method based on your case study findings, and provide insights into their practical implications in real-world scenarios. 16

14. (a) Interpret the key elements that define authentication requirements and discuss how they influence the effectiveness of authentication mechanisms. 16

(OR)

(b) Construct an analysis of the authentication applications of Kerberos and X.509, demonstrating how these protocols enhance security in distributed systems. 16

15. (a) Explain the role of IP security (IPsec) in securing a corporate network. Provide an analysis of a company that successfully implemented IPsec to protect its data transmissions, detailing the configuration choices made and the resulting impact on security. 16

(OR)

(b) Analyze a case study of a web application that faced security vulnerabilities and the measures taken to secure it. Discuss how web security protocols such as HTTPS, firewalls, and intrusion detection systems were implemented to protect against threats like SQL injection and cross-site scripting. 16