Hall Ticket No | | | | | | | | | | |

Question Paper Code: ACDC10

INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)
Dundigal-500043, Hyderabad

B.Tech VI SEMESTER END EXAMINATIONS (REGULAR) - JULY 2023
Regulation: UG-20
INFORMATION SECURITY

Time: 3 Hours **CSE (DATA SCIENCE)** **Max Marks: 70**

Answer ALL questions in Module I and II
Answer ONE out of two questions in Modules III, IV and V
All Questions Carry Equal Marks
All parts of the question must be answered in one place only

MODULE – I

1. (a) Explain the need for computer security in today's digital environment. What are the potential consequences of inadequate computer security? [BL: Understand| CO: 1|Marks: 7]

   (b) A company wants to secure their confidential documents using encryption. They are considering using either symmetric or asymmetric key cryptography. Discuss the advantages and disadvantages of each approach and provide recommendations based on different use cases. [BL: Apply| CO: 1|Marks: 7]

MODULE – II

2. (a) Discuss the step-by-step process of the Diffie-Hellman key exchange, including the generation of public and private keys. [BL: Understand| CO: 2|Marks: 7]

   (b) A message is encrypted using the Blowfish algorithm with a key of length 128 bits. If the key is known to be in hexadecimal format, what is the size of the key in bytes? [BL: Apply| CO: 2|Marks: 7]

MODULE – III

3. (a) Describe the HMAC (Hash-based Message Authentication Code) and CMAC (Cipher-based Message Authentication Code) algorithms. How do they enhance message authentication? [BL: Understand| CO: 3|Marks: 7]

   (b) Implement the Knapsack algorithm for digital signatures. Given a knapsack sequence (2, 3, 6, 13, 27, 57) and a private key (8, 19), sign a message "Hello" and verify the signature using the corresponding public key. [BL: Apply| CO: 3|Marks: 7]

4. (a) Summarize the concept of a hash function and its applications in computer security. Provide examples of popular hash functions such as secure hash algorithm (SHA) and Whirlpool. [BL: Understand| CO: 4|Marks: 7]

   (b) Design a secure authentication system for a network infrastructure using a combination of Kerberos and X.509 certificates. [BL: Apply| CO: 4|Marks: 7]

MODULE – IV

5. (a) Elucidate about (S/MIME) Secure/Multipurpose Internet Mail Extensions and its significance in securing e-mail messages. [BL: Understand| CO: 5|Marks: 7]

   (b) Implement a secure email transfer mechanism using the STARTTLS (Transport Layer Security) protocol. Explain the steps involved in negotiating a secure connection between the email client and the mail server. [BL: Apply| CO: 5|Marks: 7]

6. (a) List the components of IPsec, such as the Authentication Header (AH) and the Encapsulating Security Payload (ESP). How do they contribute to the overall security of IP communication? [BL: Understand| CO: 5|Marks: 7]

   (b) Illustrate the procedure to encrypt email message with Implement Pretty Good Privacy (PGP). Use the recipient's public key to encrypt the message and ensure that only the recipient can decrypt it using their private key. Show the step-by-step process of encryption. [BL: Apply| CO: 5|Marks: 7]

MODULE – V

7. (a) Elaborate the concepts of Secure Socket Layer (SSL) and Transport Layer Security (TLS) as protocols for secure communication over the web. [BL: Understand| CO: 6|Marks: 7]

   (b) Identify and mitigate common web vulnerabilities, such as cross-site scripting (XSS) or SQL injection attacks. [BL: Apply| CO: 6|Marks: 7]

8. (a) Classify the types of viruses and related threats that can affect web-based systems. What are the countermeasures and strategies to mitigate these threats? [BL: Understand| CO: 6|Marks: 7]

   (b) Mention the principles of firewall design and their role in protecting web systems from unauthorized access and malicious activities. Provide examples of different types of firewalls and their functionalities. [BL: Apply| CO: 6|Marks: 7]

– ∘ ∘ ◯ ∘ ∘ –