Roll No.: _

Amrita Vishwa Vidyapeetham

Amrita School of Computing, Coimbatore

B.Tech Degree Examinations – May 2024

Sixth Semester

Computer Science and Engineering

19CSE311 Computer Security

Duration: Three hours Maximum: 100 Marks

CO	**Course Outcomes**
CO01	Understand the fundamental concepts of computer security and apply to different components of computing systems.
CO02	Understand basic cryptographic techniques.
CO03	Understand how malicious attacks, threats, security and protocol vulnerabilities impact a system's Infrastructure.
CO04	Demonstrate knowledge in terms of relevance and potential of computer security for a given application.

Answer all questions

1. i. Assume that Alice wants to send a signed message to Bob using the RSA digital signature scheme. The public key parameters used by Alice are n=85 and e=7. Alice wants to sign the message m=10.

a. Identify and calculate the two prime numbers p and q that satisfy n=pq.

[CO02][BTL3][1 Mark]

b. Calculate Alice's private exponent d which is used for generating the signature.

[CO02][BTL3][1 Mark]

c. Calculate the signature ss of the message mm using the private key.

[CO02][BTL3][2 Marks]

d. Describe how Bob verifies the signature using Alice's public key. [CO02][BTL3][1 Mark]

e. Explain why it is crucial that p and q remain secrets. [CO02][BTL3][1 Mark]

ii. A network device uses a 1-byte checksum for error detection. The data packet contains the following four bytes represented in hexadecimal: 0x12, 0xAB, 0x34, and 0xCD.

a. Calculate the checksum for this packet using one's complement arithmetic.

[CO01][BTL3][2 Marks]

b. Discuss what happens if an attacker changes a message character.

[CO01][BTL3][2 Marks]

c. Explain the limitations of this checksum method. [CO01][BTL3][2 Marks]

2. i. Discuss the importance of implementing specialized database security measures within an organization, considering the complexities of DBMS, SQL vulnerabilities, the expertise gap among staff, and challenges arising from using diverse platforms. [COO3][BTL3[5 Marks]

ii. Discuss the mechanism of an SQL injection (SQLi) attack, supported by an architecture diagram that elucidates the sequence of actions an attacker employs to breach a database via SQLi. Further, give an example of a notable SQLi attack, detailing the attack's methodology and its repercussions on the victim organization. [COO3][BTL3[6 Marks]

iii. Describe how access control works in database management systems (DBMS), focusing on the role of SQL's GRANT and REVOKE commands. Include an explanation of different types of administrative policies and access rights that can be managed through these commands. Provide a specific example of how a database administrator could use the GRANT command to assign access rights, and then how they could revoke those rights using the REVOKE command. [COO3][BTL3[6 Marks]

3. i. A wants to send a mail to B within the same organization. The mail server in the organization schedules the mail delivery such that one mail is delivered after the previous mail has been read by the receiver. Illustrate the processes and agents involved in the process of A sending a mail to B. Also, If A wants to send the same mail to three recipients, how the mail server work? [CO04][BTL3][10 Marks]

ii. a. Assume Ram is a legitimate user in the Company A. He has been given the rights of a security administrator. Suddenly, when he tries to use his user login, he has been rejected for service. Identify and describe the type of attack. Suggest few prevention measures for such attacks. [CO04][BTL2][4 Marks]

b. Differentiate the three types of intruders. Assume an unauthorized person Darth is using the credential of Tom to access the system files. Identify the type of the intruder Darth. [CO03][BTL3][3 Marks]

4. i Complete the table by providing examples for trust-related challenges and strategies for building trust in social media interactions. [CO03][BTL4][5 Marks]

Particulars	Challenge	Strategy to address challenge
Trust in Information Accuracy	Misinformation, fake news, and rumors can spread rapidly on social media	
Trust in Privacy and Data Protection	Concerns about privacy breaches, data misuse	
Trust in Online Interactions	cyberbullying, harassment, or scams on social media	
Trust in Content Authenticity	Deepfakes, edited images	
Trust in Platform Policies	Transparency of social media platforms' content moderation and data practices	

ii. Imagine you are designing a trusted system for a financial institution that handles sensitive customer data and transactions. How would you ensure the system's trustworthiness in terms of data integrity, confidentiality, and availability, considering potential threats such as cyberattacks, insider threats, and system failures? Provide a comprehensive plan outlining the security measures and technologies you would implement to address these challenges and maintain the system's trustworthiness over time [CO03][BTL 4][5 Marks]

iii. For the case study done by you, analyze the key factors that contributed to the security breach/incident discuss the vulnerabilities exploited, the impact on the affected organization, and recommend proactive measures or best practices to prevent similar security incidents in the future. [CO04][BTL4][10 Marks]

5. i. With a neat block diagram explain the message exchanges in the Kerberos V4.
[CO03][BTL2][3+7 Marks]

ii. With examples illustrate how modern UNIX file system supports the Access Control Lists.
[CO04][BTL2][7 Marks]

6. i. a. Given a client and server with a secure SSL connection between them. Given the following cipher suites, identify the names of key exchange, encryption and hashing algorithms used to establish the secure connection. Explain which is the best among the following:
[CO04][BTL4][3 Marks]

a. *SSL_DH_anon_WITH_RC4_128_MD5*

b. SSL_DHE_DSS_WITH_DES_CBC_SHA

b. Given that SSL provides a secure connection between two parties, identify the service in SSL to solve the following issues: [CO03] [BTL2][5 Marks]

a. Exchange huge volumes of data between the parties efficiently.
b. Prevent modification of data in transit.
c. Ensure that no third-party will be able to understand the data being exchanged.
d. Transfer standard size data blocks to the transport layer
e. Add headers before passing to next layer

6. ii. a.Multiple users connect to an online ecommerce application and they are notified with different alert messages from the SSL layer. Group the following messages as *warnings* or *fatal errors* under the SSL Alert Protocol. [CO04] [BTL2][4 Marks]

1. Bad certificate
2. Certificate expired
3. Handshake failure
4. Bad record MAC
5. Close Notify
6. No certificate
7. Illegal parameters
8. Decompression failure

b. Suppose that a customer purchases items and is willing to make an online payment. Explain how is a dual signature generated to complete the order. [CO04] [BTL3][5 Marks]

****

Course Outcome /Bloom's Taxonomy Level (BTL) Mark Distribution Table

CO	**Marks**	**BTL**	**Marks**
CO01	**6**	2	**30**
CO02	**6**	3	**47**
CO03	**45**	4	**23**
CO04	**43**		