SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

1. Identify Threats: List possible attacks and their impact.
2. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
3. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
4. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
5. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 1: Secure Online Banking System

- A bank wants to design a secure online banking system where customers can log in, transfer money, and pay bills.
- The system must prevent phishing, session hijacking, brute force attacks, and data tampering while ensuring non-repudiation of transactions.
- The authentication and communication protocol should protect user accounts
- How would you design authentication and transaction verification to prevent the threats?

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

6. Identify Threats: List possible attacks and their impact.
7. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
8. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
9. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
10. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 2: Secure Messaging Application

- A company is developing an end-to-end encrypted messaging app.
- The goal is to protect user messages against eavesdropping, data tampering, MITM, and traffic analysis attacks.
- The protocol should also support non-repudiation to verify message senders.
- The protocol should ensure message confidentiality and integrity.

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

11. Identify Threats: List possible attacks and their impact.
12. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
13. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
14. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
15. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 3: Secure Smart Home IoT Network

- A smart home system lets users remotely control door locks, cameras, and lights via a mobile app.
- The protocol should defend against MITM, spoofing, DoS, and session hijacking attacks.
- It must ensure that only authorized users can control the devices.
- The protocol should have Secure lightweight communication between IoT devices and the server.

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

16. Identify Threats: List possible attacks and their impact.
17. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
18. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
19. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
20. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 4: Secure Medical Record System for Hospitals

- A hospital network is designing a secure electronic health record (EHR) system.
- It must prevent data tampering, unauthorized access, zero-day exploits, and malware infections.
- Only doctors and authorized personnel should access patient records, and all changes should be logged.

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

21. Identify Threats: List possible attacks and their impact.
22. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
23. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
24. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
25. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 5: Secure Government communication

A government agency wants a highly secure internal communication system to exchange classified information. The system must be resilient against zero-day exploits, malware, session hijacking, and brute-force attacks while ensuring absolute confidentiality.

- Design a Implement multi-layered security for government-level secrecy.

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

26. Identify Threats: List possible attacks and their impact.
27. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
28. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
29. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
30. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 6: Secure Online Exam System

- A university is developing an online exam platform to prevent cheating and impersonation.
- The system should protect against session hijacking, data tampering, malware, and social engineering attacks.
- Only verified students should be able to access and submit exams securely.

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

31. Identify Threats: List possible attacks and their impact.
32. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
33. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
34. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
35. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 7: Secure Online University Exam System

- A university wants to implement a secure online exam platform to prevent cheating and impersonation.
- The system should defend against session hijacking, malware, social engineering, and replay attacks.
- Additional features:
    - Students must be physically present at designated locations to take exams.
    - Detect suspicious activity (e.g., multiple people in the room).
    - Ensure exams are not leaked before the test.

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

36. Identify Threats: List possible attacks and their impact.
37. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
38. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
39. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
40. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 8: Secure National-Level Entrance Exam System

- A government is conducting a nationwide online entrance exam.
- The system must ensure secure candidate authentication and prevent large-scale cheating.
- Security measures:
    - Suggest controls to prevent traffic analysis attacks on exam servers.
    - Secure loginsto log in securely.
    - Suggest controls to prevent to detect unauthorized question paper sharing.

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

41. Identify Threats: List possible attacks and their impact.
42. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
43. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
44. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
45. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 9: Secure Online Learning Platform (e.g., Coursera, Udemy, edX)

- An online learning platform wants to prevent piracy, fake certifications, and unauthorized access.
- The system must defend against session hijacking, phishing, and malware injection.
- Security measures:
    - verification to prevent fake credentials.
    - Digital Rights Management (DRM) for course materials.
    - Controls to prevent screen recording tools from capturing courses.

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

46. Identify Threats: List possible attacks and their impact.
47. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
48. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
49. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
50. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 10: Secure Access Control System for Gas Plants

- A gas plant needs a high-security system for personnel and their devices.
- The system must prevent spoofing, insider threats, and malware attacks.
- Security measures:
    - Employees can access critical systems only within a specific time and location.
    - Strong using biometric and cryptographic keys.
    - Even authorized personnel should have minimal privileges by default.

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

51. Identify Threats: List possible attacks and their impact.
52. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
53. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
54. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
55. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 11: Secure Communication System for Law Enforcement

- A national police agency needs a secure communication network for officers in the field.
- The system must prevent MITM, eavesdropping, and insider attacks.
- Security measures:
    - Encrypted multi-hop communication to prevent traffic analysis.
    - Messages cannot be tracked/ stored after a defined time.
    - Controls to prevent stolen radios from being used.

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

56. Identify Threats: List possible attacks and their impact.
57. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
58. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
59. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
60. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 12: Secure Online Voting System

An organization is designing a secure online voting system to be used in national elections. The goal is to ensure **vote confidentiality**, **vote integrity**, and **voter authenticity**, while preventing **coercion**, **double voting**, and **vote manipulation**.
The system must defend against threats such as **insider tampering**, **replay attacks**, **MITM (man-in-the-middle)**, and **data leakage during transmission or storage**.
It should also ensure **verifiability**, allowing voters to confirm their vote was counted correctly without compromising vote secrecy.

Design a protocol or system architecture that satisfies the following requirements:

- Voter authentication and authorization without revealing the vote.
- End-to-end vote confidentiality and integrity.
- Resistance to coercion and vote selling.
- Support for public auditability and verifiability of election results.
- Scalability for large-scale elections and resilience to denial-of-service (DoS) attacks.
- votes should be verifiable

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College Of Engineering

Department of Computer Engineering

Honours in Cyber Security and Forensics

Sub: Applied Cryptography — Semester : IV

Internal Assessment Task-1 — March 18,2025

Open book Test.

Note: Use of Personal laptops, tabs, mobile phones are strictly prohibited

For each scenario, students should:

1. Identify Threats: List possible attacks and their impact.
2. Design a Security Protocol: Propose encryption, authentication, and key exchange techniques. Use cryptographic techniques, access controls, and secure communication protocols.
3. Ensure CIA (Confidentiality, Integrity, Availability): Describe how the system protects against threats.
4. Defend Against Specific Attacks: Explain how the protocol handles phishing, DoS, MITM, etc.
5. Provide Justification: Why are certain cryptographic techniques chosen?

Summary of Attacks by Category :(it's not the complete list, students may add attacks as they feel appropriate)

- Confidentiality Attacks: Eavesdropping, Traffic Analysis, MITM, Session Hijacking, Phishing, Spoofing, Onion Routing De-Anonymization.
- Integrity Attacks: Data Tampering, Replay Attacks, Non-Repudiation, Forging Digital Signatures, Malware Injection, Insider Threats, Supply Chain Tampering.
- Availability Attacks: DoS/DDoS, Brute Force, Zero-Day Exploits, Relay Attacks, Geofencing Bypass, IoT Botnet Attacks, Traffic Injection.

Problem 13 : Privacy-Preserving Biometric Authentication System

A company is building a cloud-based biometric authentication system to be used in critical infrastructure access control (e.g., airports, nuclear facilities, government buildings).
The system uses **biometric identifiers** such as fingerprints, iris scans, or facial recognition for verifying user identity.
The goal is to ensure **user privacy**, **template integrity**, and **authentication reliability**, while defending against **template leakage**, **spoofing attacks**, and **insider threats**.
The system must also support **revocability** in case a biometric template is compromised.

Design a protocol or architecture that satisfies the following requirements:

- Secure storage and matching of biometric data without exposing raw templates.
- Resistance to biometric spoofing and replay attacks.
- Mechanism for cancelable biometrics (support for reissuance without losing uniqueness).
- Privacy-preserving techniques
- Compliance with data protection regulations (e.g., GDPR) and support for user consent.