



COMSATS University Islamabad (CUI)

Department of Computer Science

Terminal Examination spring -2024

BSAI, BSSE, BCS, BSDS

Course: CSC432-Information Security

Maximum Marks: 50

Instructors: Dr. AbdulRahman Al-Salehi, Ms. Sara Ali, Ms. Haseena Kainat

Dated: January 2025

Time Allowed: 3 hours

- All questions are self-explanatory and require no further explanations during exam time.
- Return the question paper along with the answer sheet.
- Attempt all questions.

-----CLO-1-----
(Discuss the fundamental concepts, policies, standards, and ethical issues of information security.)

Question 1:

[2+2+2+2=8 marks]

- Explain the concepts of confidentiality, integrity, and availability (CIA triad) in cryptography. How do they complement each other to ensure secure communication? Can one aspect be compromised while the others remain intact?
- Describe an illustrative representative example situation in which confidentiality compromise also causes integrity compromise.
- As a role of Chief Information Security Officer (CISO), you are tasked with implementing measures to deter illegal, immoral, or unethical behavior and protect the organization's information systems. Based on the scenario, what do you identify as the potential causes of unethical and illegal behavior within the organization, and how do each of these causes contribute to such actions within an organization?
- Compare biometric authentication with two-factor authentication (2FA). How does each method contribute to securing user identities?

-----CLO-2-----
(Investigate various counter measures and security controls to minimize risk and exposure)

Question 2:

[4+6+3=13 marks]

- An e-commerce website faces an average of 3 DDoS attacks per year. Each attack results in 6 hours of downtime, costing \$500 per hour in lost revenue and mitigation expenses. Calculate the Annual Loss Expectancy (ALE) for these attacks.
- ABC Manufacturing Company is developing a new product line with projected revenues of \$500,000. Using the following table, calculate the ARO and ALE for each potential risk category as shown in the table (supply chain disruptions, equipment failure, and regulatory fines).

Risk Category	ARO (Annual Rate of Occurrence)	SLE (Single Loss Expectancy)	ALE (Annual Loss Expectancy)
Supply Chain Disruption	2	\$50,000	?
Equipment Failure	1	\$75,000	?
Regulatory Fines	0.5	\$100,000	?

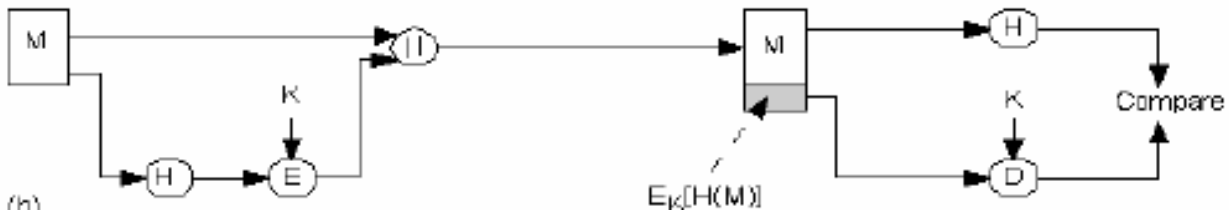
- c) Describe how the various types of firewalls interact with the network traffic at various levels of the OSI model.

-----CLO-3-----
(Analyze various information security technologies)

Question 3:

[4+3+4+4+3+4= 22 marks]

- a) Consider the following 8-bit block of data: 11010101. Apply the Initial Permutation (IP) of **DES** on the given 8-bit block. The IP is defined as: $IP=(2,6,3,1,4,8,5,7)$. This means the first bit goes to position 2, the second bit goes to position 6, and so on. Bit positions start from 1. After applying the initial permutation, what is the resulting 8-bit block?
- b) Based on the figure given below, explain whether the model ensures confidentiality, integrity, or authentication, and justify your answer.



- c) Alice and Bob are using the Diffie-Hellman key exchange protocol with the following parameters:
- Prime $p=23$
 - Generator $g=5$
- Alice chooses her private key $a=6$, and Bob chooses his private key $b=15$.
1. Calculate the public keys for Alice and Bob.
 2. Compute the shared secret key.
- d) Explain how can you use Least Significant Bit method in steganography by the following example: Data to be inserted: character **Z** .
Host pixels: 3 pixel [00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111 11101001]. Also explain how the data is extracted by the receiver. (ASCII value for Z is 90).
- e) The company's financial department prepares quarterly reports and sends them to external auditors for verification. These reports contain critical business data that needs to remain confidential, accurate, and untampered with during transmission. The reports are sent via email, and auditors need to verify that the report they receive is indeed from your company, and that the contents haven't been altered. You have implemented an asymmetric encryption system for this purpose, where the company has a private key and each auditor has the public key.
1. How would you set up the digital signature process for the financial reports to ensure the auditors can verify the authenticity of the reports?
 2. What steps should auditors follow to verify the authenticity of the financial report they receive?
 3. What potential risks could occur if the private key is compromised, and how could you mitigate these risks?
- f) Alice is visiting an e-commerce website to make an online purchase. Her browser shows a padlock icon, indicating the connection is secure. Provide very precise and brief answers.
1. What is a digital certificate, and why is it important in this scenario?

2. What risks does Alice face if the digital certificate is fraudulent or untrustworthy?
3. How can Alice verify the legitimacy of the website using the digital certificate?
4. How does a Certificate Authority (CA) authenticate the digital certificate?

-----CLO-4 -----
(Describe the policies and procedures to information security implementation and maintenance)

Question 4:

[3+4= 7 marks]

- a)** By taking into consideration the different US laws and procedures, identify the attack and briefly explain is the below mentioned attack legal or illegal. What is the penalty in case of being caught?
In 2000, a 15-year-old hacker known as ‘Mafiaboy’ took down several major websites including CNN, Dell, E-Trade, eBay, and Yahoo!, the last of which at the time was the most popular search engine in the world. This attack had devastating consequences, including creating chaos in the stock market. Mafiaboy, who was later revealed to be a high schooler named Michael Calce, coordinated the attack by compromising the networks of several universities and using their servers to conduct the attack. The aftermath of this attack directly led to the creation of many of today’s cybercrime laws.
- b)** In a cybercrime investigation, law enforcement seizes digital devices (laptops, hard drives, and phones) from suspects involved in a large-scale financial fraud affecting multiple banks. Forensic investigators recover and analyze digital evidence to identify the perpetrators and understand the fraud. Outline the key steps in the digital forensics methodology and explain how each step would be applied in the investigation.

Best of Luck
