Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING
MID TERM EXAMINATION - OCT 2023

Semester : Semester V - 2021
Course Code : CSE3078
Course Name : Sem V - CSE3078 - Cryptography and Network Security
Program : B. TECH

Date : 30-OCT-2023
Time : 2:00PM - 3:30PM
Max Marks : 50
Weightage : 25%

Instructions:
(i) Read all questions carefully and answer accordingly.
(ii) Question paper consists of 3 parts.
(iii) Scientific and non-programmable calculator are permitted.
(iv) Do not write any information on the question paper other than Roll Number.

PART A

ANSWER ALL THE QUESTIONS **(5 X 2 = 10M)**

1. Define Cryptography.

(CO1) [Knowledge]

2. The Vernam method is used to encrypt the plain text 's,' represented in binary as 01110011, with a key '$,' represented as 00100100. Calculate the resulting cipher text using this encryption method.

(CO1) [Knowledge]

3. List out the problems of one time pad.

(CO1) [Knowledge]

4. Which cryptosystem should Jake employ to secure the private message Megan wants to send him? To guarantee that only Jake can decipher the message, he opts to use Megan's public key for encryption. How many key pairs will be required by each of them for this secure communication?

(CO2) [Knowledge]

5. In block ciphers, the concept of confusion is fundamental, aiming to create a intricate relationship between the ciphertext and the encryption key. To maximize this confusion, a complex substitution algorithm is commonly employed. Identify the specific component within DES (Data Encryption Standard) responsible for creating the highest level of confusion.

(CO2) [Knowledge]

PART B

ANSWER ALL THE QUESTIONS **(4 X 5 = 20M)**

6. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

1. A major social media platform experiences a security breach when a group of hackers discovers a vulnerability in the platform's authentication system. They gain unauthorized access to numerous user accounts, altering profile information, posting offensive content, and spreading false information on behalf of the compromised users.
2. A prestigious research university's database containing groundbreaking scientific research is targeted by cybercriminals. They successfully breach the university's network and exfiltrate confidential research data, including experimental results, formulas, and prototypes. The cybercriminals later demand a ransom in exchange for not publishing the research findings.
3. A popular online gaming platform faces a Distributed Denial of Service (DDoS) attack during a highly anticipated game release event. The attack overwhelms the platform's servers, causing a complete shutdown for several hours. Gamers worldwide are unable to access their accounts and engage in the new game, leading to severe dissatisfaction and financial losses for the company.
4. A healthcare organization faces an insider threat when an employee accesses patient records without authorization, altering some medical diagnoses. This breach impacts both patient privacy and data integrity.
5. A large technology company experiences a cyberattack where an attacker gains access to confidential employee data and introduces malware into the network, causing disruptions in service.

(CO1) [Comprehension]

7. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

1. A leading e-commerce website, known for its strict security measures, suffers a data breach when an insider with privileged access credentials leaks sensitive customer data, including credit card information, to a group of malicious actors.
2. A well-known healthcare institution's network falls victim to a ransomware attack. The attackers encrypt critical patient records, including medical histories and diagnostic reports, and demand a significant ransom for the decryption key, disrupting patient care.
3. A financial institution experiences an elaborate cyberattack where hackers manipulate the stock trading system, causing stock prices to fluctuate erratically. Investors suffer substantial financial losses, and the stock market's integrity is compromised.
4. A government agency encounters a sophisticated espionage attack as foreign agents gain unauthorized access to classified documents, potentially exposing sensitive national security information.
5. A prominent news organization's website is targeted by cybercriminals who deface articles and replace them with false and misleading information. Readers are misled by the manipulated content, impacting the organization's credibility.

(CO1) [Comprehension]

8. Using the Playfair Cipher, decrypt the given cipher text into its equivalent plaintext using the following information:
Cipher Text: **RYMIGQRMHQQRMGQORMECRMCXNUIBTGWETZ**
Key: **SPREAD SPECTRUM**
Filler Text: ***X***

1. Complete the **Polybius matrix** [**2 Marks]**
2. Show the transformation by creating a table with rows for cipher text digraphs, and resulting plaintext.[3 **Marks]**

(CO2) [Comprehension]

9. 1. Imagine you're responsible for the cybersecurity of a medium-sized business. You receive a report that some of your employees have fallen victim to a phishing email campaign. The attackers gained access to sensitive company information, including financial data. Explain whether this situation is an example of an active attack, a passive attack, or a combination of both. Justify your answer and outline immediate steps you would take to mitigate this threat

2. You are an IT security analyst at a financial institution. Recently, you detected that an intruder has been actively scanning your network, attempting to exploit vulnerabilities. Fortunately, your security measures have so far prevented unauthorized access. Describe the type of active attack this scenario represents and explain how you would respond to it. Additionally, discuss any specific countermeasures you might employ to enhance your network's security against such attacks.

(CO1,CO2) [Comprehension]

PART C

ANSWER THE FOLLOWING QUESTION **(1 X 20 = 20M)**

10. 1. Decrypt this encrypted message using **Rail Fence Cipher**. Show All Steps.**[5 Marks]**
Key: 5
Encrypted message: CANSYOENUINSTXMMSMCOEIXSCCMAICRXEOTUX

2. Using the **Columnar Transposition Cipher**, decrypt the given cipher text into its equivalent plaintext using the following:**[5 marks]**
Cipher Text: MICOHLCAAGPYMAYHACIGTITXTANREMRP
Key: ELSEVIER
Pad : X
a. Complete the table below showing the key and cipher text in columnar format.
b. Perform 1 round of transformation only.
c. Write the resulting plain text in the below table.

3. Eve captures Bob's Hill cipher machine, which uses a 2-by-2 matrix M mod 26. She tries to attack. She finds that the cipher is APADJ TFTWLFJ and the key is HILL.
What is the Plain Text ? (10 Marks)

(CO4,CO2,CO1,CO3) [Application]