



Department of Computer Science and Engineering
Cryptography and Network Security(22CS401)

Module-1 Question Bank

III YEAR CSE

Section-10

Question-1

A university's student portal experiences security issues where an attacker secretly monitors network traffic (passive attack) and alters stored student data (active attack). To protect the system, the security team applies core **computer security concepts** such as confidentiality, integrity, and availability. They implement **security services** like authentication, integrity protection, and confidentiality, supported by **security mechanisms** such as encryption, hashing, access control, and firewalls to secure the portal from further attacks.

- A. Identify the passive and active attacks present in the student portal scenario
- B. Apply suitable security services and mechanisms to protect a university student portal from passive and active attacks, ensuring confidentiality, integrity, and availability.
- C. Analyze how the active attack on student data impacts the security services required for the portal.

Question-2

A company's network exchanges sensitive information between users and a central server. To protect these communications, the system uses various security measures to ensure that data is sent safely and reaches the correct recipient without alteration. However, an intruder on the network attempts to intercept or change the messages during transmission. To defend against this, the system applies methods that verify user identity, prevent unauthorized access, and ensure that messages remain confidential and unchanged.

- A. Describe the ways protective measures in the scenario ensure safe communication between users and the server.
- B. Select an appropriate technical approach that can prevent the intruder from reading the transmitted information and describe how it works
- C. Analyze how the intruder's attempt to alter messages affects the reliability of the communication process.

Question-3

A company sends sensitive information between employees and servers over its internal network. To protect these messages, the system uses several security components that work together during transmission. An intruder on the network may try to read, modify, or block the data. To prevent this, the communication process applies protective methods using algorithms, keys, and supporting services to ensure the message reaches the intended receiver securely.

- A. Describe the role each component plays in ensuring that messages reach the intended receiver securely.
- B. Select one component from the scenario and apply it to protect a message from unauthorized access.
- C. Analyze how the failure of any one component (such as a key or algorithm) would impact the overall security of the communication process.

Question-4

A research team in a university exchanges short confidential messages related to project work. To protect the information, they decide to use the Playfair technique, where each pair of letters in the message is substituted using a 5×5 key matrix generated from a shared keyword. Only team members who know the keyword can decode the message. An attacker intercepts some encrypted text and attempts to break the pattern by studying repeating digraphs and their positions. The team must ensure the chosen keyword and matrix structure make it difficult for the attacker to reconstruct the original message.

A. Describe how the plaintext “COMMUNICATION” would be processed for encryption using the Playfair cipher with the key square COMPUTER, and state how a letter pair such as “CO” is handled when both letters appear in the same row or column of the key square.

B. Using the key “KEYWORD”, construct the Playfair key square and apply it to encrypt the plaintext “ATTACK AT DAWN”, then use the same key square to decrypt the ciphertext “BMODZBMXA” by processing each digraph step by step.

C. Analyze the strengths and weaknesses of the Play fair cipher compared to the Caesar cipher, highlighting its use of digraphs versus single-letter shifts.

Question-5

A financial organization needs to secure short transaction codes exchanged between its employees. To strengthen confidentiality, the organization uses the Hill cipher, where each block of letters in the message is converted into numerical vectors and multiplied with a secret key matrix known only to authorized staff. The resulting encrypted vectors are converted back to letters and sent over the network. An attacker intercepts some encrypted messages and attempts to determine the key matrix by analyzing repeated blocks. The security team must select a key matrix with strong invertibility properties to prevent the attacker from reconstructing the original transaction codes.

A. Describe how the Hill cipher uses matrix multiplication during encryption and explain the role played by the key matrix in this process.

B. Using the given key “HILLMAGIC” encrypt the plaintexts “GFG” and “ACT” with the Hill cipher—show all matrix calculations and the resulting ciphertext.

C. Compare and contrast brute-force attacks, frequency analysis, and differential cryptanalysis as methods of breaking encryption”

Question-6

A research team in a university exchanges confidential project data between laboratories over the campus network. To protect the information, they decide to use the Data Encryption Standard (DES), a symmetric key encryption algorithm, where the message is divided into 64-bit blocks and encrypted using a shared 56-bit secret key. Each block undergoes 16 rounds of Feistel operations, including expansion, substitution using S-boxes, permutation, and XOR operations with round keys, transforming the plaintext into ciphertext. Only team members who possess the secret key can decrypt and access the original data. An attacker intercepts the encrypted communication and attempts to break it through brute-force or cryptanalytic analysis, but the complexity of multiple rounds and key-dependent transformations makes reconstructing the original message difficult, emphasizing the importance of secure key selection and management.

a.State the basic features of the DES algorithm and list the steps involved in generating the 16 subkeys used in DES encryption.

B.Encrypt the plaintext "VIGNANCSE" using DES with a given key, showing each step of the process.

C.Analyze DES by comparing its 56-bit key length with the 128-, 192-, and 256-bit key lengths of AES, and examine the resulting strengths and weaknesses of DES in terms of security under modern encryption standards.

Question-7

A university data center needs to securely store and share sensitive information such as student records, research files, and payroll data across its internal network and cloud systems. To protect this information from unauthorized access and potential attacks, the IT team adopts the **Advanced Encryption Standard (AES)** as the encryption mechanism. By encrypting the data before storage and transmission, the university ensures that even if the information is intercepted or accessed by an attacker, it remains unreadable without the correct secret key, making AES a reliable choice for modern network security

A.List the main steps involved in the AES encryption process and outline how the round keys used in AES encryption are generated.

B.Decrypt the cipher text "A1B2C3D4" using AES with a given key, showing each step of the process.

C.Compare AES to DES,for each of the following elements of DES,indicate the comparable element in AES or explain why it is not needed in AES.

- i) XOR of subkey material with the input to the f function
- ii) XOR of the f function output with the left half of the block
- iii) F function
- iv) Permutation P
- v) Swapping of halves of the block

Question-8

A university research and academic portal supports online services and secure collaboration between students, faculty, and research teams over a public network. Since the users do not initially share a secret key and the communication channel is insecure, the system first uses the Diffie–Hellman key exchange algorithm to allow the communicating parties to securely establish a shared secret session key. To ensure authentication and protect sensitive information such as login credentials, research data, and internal communications, the portal also employs the RSA public key cryptosystem, where public and private keys are used to encrypt data and verify identities. By combining Diffie–Hellman for secure key establishment and RSA for encryption and authentication, the university ensures confidential and trusted communication even in the presence of potential eavesdroppers.

- A. State the main steps involved in the RSA encryption and decryption process.
- B. Demonstrate encryption and decryption using the RSA algorithm, for the following:
 - a. $p = 3; q = 7, e = 5; M = 10$
 - b. $p = 17; q = 23, e = 9; M = 7$
- C. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q=353$ and a primitive root $a=3$
 - i) if Alice has a private key $X_A=97$, find her public key Y^A
 - ii) If Bob has a private key $X^B=233$, find his public key Y^B
 - iii) What is the shared secret key between Alice and Bob

Question-9

A university information system manages sensitive data such as student records, examination results, and research submissions. To ensure data integrity and authenticity, the system uses cryptographic hash functions. Whenever a file or message is stored or transmitted, the system generates a fixed-length hash value for the data and stores or shares it along with the original content. When the data is accessed or received, the hash is recomputed and compared with the original hash to detect any unauthorized modification. Even a small change in the data produces a completely different hash value, making it easy to identify tampering. This approach helps the university verify data integrity, support secure password storage, and maintain trust in digital communication.

- A. List common Message Authentication Code (MAC) algorithms such as HMAC, CMAC, and UMAC, and outline how a MAC helps detect accidental changes and intentional tampering of a message.
- B. Given a message "**CONFIDENTIAL**" and its corresponding MAC value, verify the MAC using the **HMAC-SHA512** algorithm with a provided key.
- C. Analyze how MACs protect against various types of attacks, such as replay attacks or forgery.

Question-10

A university administration system regularly exchanges important digital documents such as examination results, certificates, official notices, and approval letters with students, faculty, and external agencies over the internet. To ensure that these documents are authentic, unaltered, and non-repudiable, the university adopts the Digital Signature Standard (DSS) based on the DSA algorithm. Before sending a document, the sender generates a digital signature using their private key, and the receiver verifies the signature using the sender's public key. This mechanism ensures that the document truly originates from the authorized sender and has not been modified during transmission.

A.State the purpose of the Digital Signature Standard (DSS) and outline how digital signatures provide authentication and integrity.

B.Generate and verify a digital signature for a given message using the Digital Signature Standard, showing the main steps involved.

C.Analyze how the Digital Signature Standard ensures authenticity, integrity, and non-repudiation in electronic document exchange, and discuss the impact if the private key is compromised.