Computer Network Security (IAE - 1)

▼ **Table of Contents:**

Q1: Enlist Properties & Applications of Hash Function (2 marks)

Properties of Hash Functions:

1. Fixed Output Size:

- Produces fixed-length output regardless of input size
- Common sizes: 160 bits (SHA-1), 256 bits (SHA-256)

2. Deterministic:

- Same input always produces same output
- No randomness in computation

3. Pre-image Resistance (One-way):

- Computationally infeasible to find input from hash value
- Given h, hard to find x such that H(x) = h

4. Second Pre-image Resistance:

- Hard to find different input with same hash
- Given x, hard to find $y \neq x$ such that $H(x) = H(y)$

5. Collision Resistance:

- Hard to find any two different inputs with same hash
- Hard to find x, y where $x \neq y$ and $H(x) = H(y)$

Applications of Hash Functions:

1. Digital Signatures:

- Hash message before signing for efficiency
- Ensures integrity and authenticity

2. Message Authentication Codes (MAC):

- HMAC construction for message authentication
- Combines hashing with secret key

3. Password Storage:

- Store hashed passwords instead of plaintext
- Prevents password disclosure

4. Digital Forensics:

- File integrity verification
- Evidence authentication

5. Blockchain Technology:

- Mining process and block linking
- Transaction verification

Q2: What are block cipher modes? Describe any two in detail (5 marks)

Block Cipher Modes are methods of operation that allow block ciphers to encrypt messages longer than the block size securely. Each mode has different properties regarding security, parallelization, and error propagation.

List of 5 Block Cipher Modes:

→ Electronic Codebook (ECB) Mode

→ Cipher Block Chaining (CBC) Mode

→ Cipher Feedback (CFB) Mode

→ Output Feedback (OFB) Mode

→ Counter (CTR) Mode

1. Electronic Code Book (ECB) Mode:

- **Operation**: Each plaintext block is encrypted independently using the same key
- **Encryption**: $C_1 = E(K, P_1)$, $C_2 = E(K, P_2)$, ..., $C_n = E(K, P_n)$
- **Decryption**: $P_1 = D(K, C_1)$, $P_2 = D(K, C_2)$, ..., $P_n = D(K, C_n)$
- **Advantages**: → Simple implementation,
  → parallel processing possible,
  → no error propagation.
- **Disadvantages**: → Identical plaintext blocks produce identical ciphertext blocks,
  → patterns visible,
  → not secure for large data

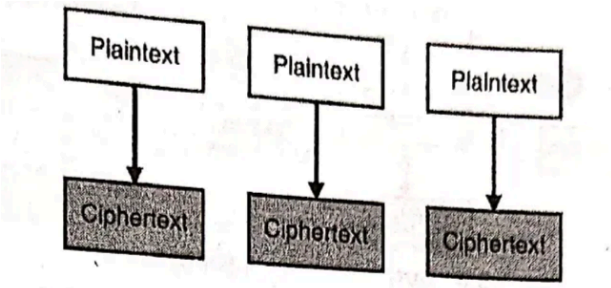


Fig. 2.5.3 : Electronic Code Book (ECB) Mode

2. Cipher Block Chaining (CBC) Mode:

- **Operation**: Each plaintext block is XORed with the previous ciphertext block before encryption
- **Encryption**: $C_1 = E(K, P_1 \oplus IV)$, $C_i = E(K, P_i \oplus C_{i-1})$
- **Decryption**: $P_1 = D(K, C_1) \oplus IV$, $P_i = D(K, C_i) \oplus C_{i-1}$
- **Advantages**: → Identical plaintext blocks produce different ciphertext,
  → more secure than ECB
- **Disadvantages**: → Sequential encryption,
  → error propagation,
  → requires initialization vector (IV)

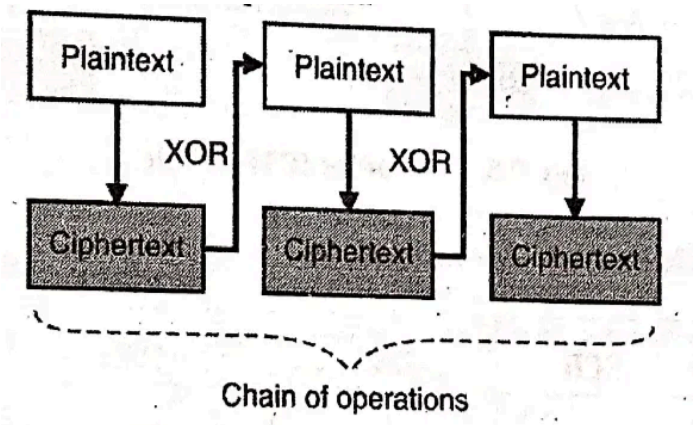


Fig. 2.5.4 : Cipher Block Chaining (CBC) Mode

Q3: Compare and Contrast DES & AES (5 marks)

Parameter	DES (Data Encryption Standard)	AES (Advanced Encryption Standard)
Block Size	64 bits	128 bits
Key Size	56 bits (64 bits with parity)	128, 192, or 256 bits
Rounds	16 rounds	10, 12, or 14 rounds (depending on key size)
Structure	Feistel Network	Substitution-Permutation Network
Development	Developed by IBM (1975)	Developed by Rijmen & Daemen (2001)
Security	Vulnerable to brute force attacks	Highly secure, no practical attacks
Speed	Slower in software	Faster in both software and hardware
Key Schedule	Simple key schedule	Complex key expansion

Key Differences:

- **Security Level**: AES is significantly more secure due to larger key sizes
- **Performance**: AES is more efficient and faster
- **Flexibility**: AES supports multiple key sizes, DES has fixed key size
- **Current Status**: DES is obsolete, AES is current standard

Compare HMAC & CMAC (5 marks)

Parameter	HMAC (Hash-based MAC)	CMAC (Cipher-based MAC)
Base Algorithm	Uses hash functions (SHA-1, SHA-256)	Uses block ciphers (AES, DES)
Input	Works with any hash function	Works with any block cipher
Key Usage	Uses two keys (inner and outer)	Uses single key

Parameter	HMAC (Hash-based MAC)	CMAC (Cipher-based MAC)
Structure	HMAC(K,M) = H((K⊕opad) || H((K⊕ipad) || M))	Based on CBC mode with special processing
Security	Security depends on hash function	Security depends on underlying cipher
Performance	Generally faster	Slower than HMAC
Standardization	RFC 2104, FIPS 198	NIST SP 800-38B

Key Differences:

- **Algorithm Basis**: HMAC uses cryptographic hash functions, CMAC uses block ciphers
- **Key Management**: HMAC uses key derivation, CMAC uses direct key application
- **Efficiency**: HMAC is typically more efficient for software implementations

Q4: Describe RC5 Algorithm with an example (5 marks)

Definition

RC5 is a **symmetric key based block cipher** designed by **Ronald Rivest in 1994**. RC stands for "Rivest Cipher" or "Ron's Code".

Key Features

RC5 has **three variable parameters**:

- **Block size (w)**: 32, 64, or 128 bits
- **Key size**: 0 to 2040 bits (variable length)
- **Number of rounds (r)**: 0 to 255 rounds

Algorithm Structure

- RC5 works with **two w-bit words** (A and B)
- Uses an **expanded key table S** with t = 2(r+1) words
- Nominal choice: w = 32 bits (giving 64-bit block size)

Key Expansion Process

Three steps:

1. Convert secret key from bytes to words
2. Initialize array S with magic constants
3. Mix in the secret key

Encryption Algorithm

```
A = A + S[0]
B = B + S[1]
for i = 1 to r do:
  A = ((A XOR B) <<< B) + S[2*i]
  B = ((B XOR A) <<< A) + S[2*i + 1]
```

Example

Parameters:

- w = 32 bits, r = 2 rounds
- Key = "KEY" (24-bit key)

Process:

1. **Plaintext**: Split into two 32-bit words A and B
2. **Initial operations**:
   - A = A + S
   - B = B + S
3. **Round operations**: Apply XOR, rotation, and addition operations for r rounds
4. **Output**: Final values of A and B form the ciphertext

Advantages

- **Flexible parameters** for different security requirements
- **Simple operations** (XOR, addition, rotation)
- **Fast performance** in both software and hardware
- **Variable security levels** based on chosen parameters

The algorithm's strength comes from its variable parameters and the combination of simple but effective operations that create strong diffusion and confusion properties.

Q5: Explain public key cryptography & RSA algorithm.
RSA Problem - Given modulus n=91, public key e=5, find value of φ(n) and d using RSA encrypt M=25 (5 marks)

Public Key Cryptography & RSA Algorithm

→ Public Key Cryptography

Definition: Public key cryptography is a cryptographic scheme that uses two mathematically related keys - a **public key** and a **private key** - for providing various cryptographic services.

Key Principles of Public Key Cryptosystems

1. **Asymmetric Keys**: Uses two mathematically related keys that form a key pair
2. **Public Key Distribution**: Public keys are widely known and distributed openly
3. **Private Key Security**: Private key is kept secret with its owner
4. **Mathematical Relationship**: The two keys are mathematically related but one cannot be derived from the other
5. **Encryption/Decryption**: Any key in the pair can be used for encryption, with the corresponding key used for decryption

Advantages of Public Key Cryptography

- **Easy Key Distribution**: No need for secure key exchange channels
- **Scalability**: For n users, only 2n keys are needed (compared to n(n-1)/2 for symmetric)
- **Multiple Security Services**: Provides confidentiality, authentication, and non-repudiation
- **No Prior Key Sharing**: Parties can communicate securely without prior key exchange

→ RSA Algorithm

RSA (Rivest-Shamir-Adleman) is an asymmetric key algorithm based on the mathematical difficulty of factoring large prime numbers.

RSA Algorithm Steps

1. **Choose two prime numbers**: Select two random large prime numbers p and q where $p \neq q$
2. **Calculate modulus**: $n = p \times q$
3. **Calculate Euler's totient**: $\varphi(n) = (p-1)(q-1)$
4. **Choose public exponent**: Select e such that $\gcd(e, \varphi(n)) = 1$ and $1 < e < \varphi(n)$
5. **Calculate private exponent**: $d = e^{-1} \bmod \varphi(n)$ or $ed \equiv 1 \pmod{\varphi(n)}$
6. **Key Formation**:
    - **Public Key**: $\{e, n\}$
    - **Private Key**: $\{d, n\}$
7. **Encryption**: $C = M^e \bmod n$
8. **Decryption**: $M = C^d \bmod n$

→ Numerical Solution

Given: n = 91, e = 5, **M = 25**

Step 1: Find p and q

Since n = 91, factorize: 91 = 7 × 13

Therefore: **p = 7, q = 13**

Step 2: Calculate φ(n)

φ(n) = (p-1)(q-1) = (7-1)(13-1) = 6 × 12 = **72**

Step 3: Find d using Extended Euclidean Algorithm

We need d such that: 5d ≡ 1 (mod 72)

Index i	Quotient q	Remainder r	s	t
0	-	72	1	0
1	-	5	0	1
2	14	2	1	-14
3	2	1	-2	29
4	2	0	-	-

Re-swapping values: x = 29, y = -2

Verification: 5 × 29 = 145 ≡ 1 (mod 72)

Therefore: **d = 29**

Step 4: Encryption of M = 25

C = M^e mod n = 25^5 mod 91

Calculate step by step:

- 25^1 mod 91 = 25
- 25^2 mod 91 = 625 mod 91 = 79
- 25^4 mod 91 = 79^2 mod 91 = 6241 mod 91 = 53
- 25^5 mod 91 = (25^4 × 25^1) mod 91 = (53 × 25) mod 91 = 1325 mod 91 = **51**

Final Results:

- **p = 7, q = 13**
- **φ(n) = 72**
- **d = 29**
- **Encrypted message C = 51**

Verification (Decryption):

M = C^d mod n = 51^29 mod 91 = 25 √

The RSA algorithm successfully encrypts the plaintext **M = 25** to ciphertext **C = 51** using the derived keys.

Q6. Write Short Notes on :
Explain different modes of operation of block ciphers / Block Cipher Modes of Operation / What are block cipher modes. Describe any two in detail (5 Marks)

6a. Block Cipher Modes of Operation (5 marks)

Definition: Block cipher modes define how block ciphers encrypt data larger than the cipher's block size.

Five Standard Modes:

1. Electronic Codebook (ECB)

- **Operation**: Each block encrypted independently
- **Advantages**: Simple implementation, parallel processing
- **Disadvantages**: Pattern leakage, identical blocks produce identical ciphertext
- **Use**: Single block encryption only

2. Cipher Block Chaining (CBC)

- **Operation**: Each plaintext block XORed with previous ciphertext
- **Formula**: Ci = E_K(Pi ⊕ Ci-1)
- **Advantages**: Hides patterns, semantic security
- **Disadvantages**: Sequential encryption, error propagation
- **Use**: General-purpose block-oriented transmission

3. Cipher Feedback (CFB)

- **Operation**: Block cipher used as stream cipher
- **Advantages**: Stream processing, no padding required
- **Disadvantages**: Error propagation, sequential encryption
- **Use**: Stream-oriented transmission

4. Output Feedback (OFB)

- **Operation**: Encrypt previous cipher output
- **Advantages**: No error propagation, stream processing
- **Disadvantages**: Sequential operation, vulnerable to bit-flipping
- **Use**: Noisy communication channels

5. Counter (CTR)

- **Operation**: Encrypt counter values, XOR with plaintext
- **Advantages**: Full parallelization, random access
- **Disadvantages**: Counter management, key reuse vulnerability
- **Use**: High-speed applications, parallel processing

6b. HMAC & CMAC (5 Marks)

→ Hash-based Message Authentication Code (HMAC)

Definition: Cryptographic technique ensuring data integrity and authenticity using hash function and secret key.

Algorithm:

`HMAC = H((K ⊕ opad) || H((K ⊕ ipad) || message))`

Where:

- H = cryptographic hash function
- K = secret key

- opad = outer padding (0x5C repeated)
- ipad = inner padding (0x36 repeated)

Features:

- Uses any cryptographic hash (MD5, SHA-1, SHA-256)
- Provides both authentication and integrity
- Resistance to cryptanalysis attacks
- Widely used in TLS, SSH, IPsec protocols

→ Cipher-based Message Authentication Code (CMAC)

Definition: MAC based on block cipher algorithms (AES, Triple DES).

Process:

- Message divided into blocks
- Uses block cipher in CBC-like mode
- Final block processed with special keys K1/K2
- Produces fixed-length MAC output

Key Features:

- Based on approved block ciphers (AES preferred)
- Overcomes limitations of older DAA algorithm
- Provides message authenticity and integrity
- NIST approved algorithm

6c. SHA-256 & SHA-512 (5 Marks)

→ SHA-256 (Secure Hash Algorithm 256-bit)

Technical Specifications:

- **Hash Length**: 256 bits (32 bytes)
- **Block Size**: 512 bits
- **Word Size**: 32 bits
- **Rounds**: 64 compression rounds
- **Security Level**: 128 bits

Key Features:

- Part of SHA-2 family

- Optimized for 32-bit architectures
- Widely adopted in blockchain (Bitcoin)
- FIPS 180-4 approved
- Collision resistant (no known attacks)

Applications:

- Digital signatures and certificates
- TLS/SSL protocols
- Cryptocurrency mining
- Data integrity verification

→ SHA-512 (Secure Hash Algorithm 512-bit)

Technical Specifications:

- **Hash Length**: 512 bits (64 bytes)
- **Block Size**: 1024 bits
- **Word Size**: 64 bits
- **Rounds**: 80 compression rounds
- **Security Level**: 256 bits

Performance Characteristics:

- Faster on 64-bit systems than SHA-256
- Slower on 32-bit architectures
- Higher memory requirements
- Better diffusion properties

Security Advantages:

- **Higher Collision Resistance**: 2^256 vs 2^128
- **Future-proof**: Resistant to quantum computing advances
- **Enhanced Security Margin**: Longer hash provides buffer
- **Government Applications**: Preferred for classified information

Public Key Cryptography:

- **Concept**: Uses pair of keys (public and private)
- **Public Key**: Known to everyone, used for encryption
- **Private Key**: Known only to owner, used for decryption

- **Key Algorithms**: RSA, ECC, Diffie-Hellman
- **Applications**: Digital signatures, key exchange, secure communications
- **Advantages**: Solves key distribution problem, enables non-repudiation

Q7. Describe different block cipher modes

Refer to Q6 OR Q2.

Q8.. Compare & Contrast DES & AES.

Refer to Q3.

Q9. SHA Provides Better Security than MD5 — Justify

Security Vulnerabilities Comparison:

MD5 Vulnerabilities:

- **Hash Length**: Only 128 bits → 64-bit collision resistance (broken)
- **Collision Attacks**: Two different inputs can produce same hash (2^64 operations)
- **Rainbow Table Attacks**: Pre-computed hash lookups possible
- **Cryptographically Broken**: Not suitable for security applications since 2008

SHA Family Advantages:

- **SHA-1**: 160-bit output, requires 2^80 operations for collision (deprecated)
- **SHA-256**: 256-bit output → 128-bit collision resistance (secure)
- **SHA-512**: 512-bit output → 256-bit collision resistance (very secure)

Technical Justifications:

1. Algorithm Complexity:

- **MD5**: Simple structure, vulnerable to differential cryptanalysis
- **SHA-2 Family**: More complex structure with additional security rounds
  - SHA-256: 64 rounds of processing
  - SHA-512: 80 rounds of processing

2. Resistance to Attacks:

- **Length Extension Attacks**: SHA provides better resistance
- **Semi-freespace Cryptanalysis**: SHA algorithms more resilient
- **Future-proofing**: Longer hash lengths resist quantum computing threats

3. Current Status:

- **MD5**: Deprecated and broken
- **SHA-256/SHA-512**: Industry standard, no known practical vulnerabilities

Q10. Explain the OSI Security Architecture and Network Security Model (5 marks)

→ The **OSI Security Architecture**, defined by ITU-T X.800 standard, provides a systematic framework for implementing security at each layer of the OSI model.

Definition: OSI Security Architecture is a systematic approach that defines security requirements and specifies means by which these requirements can be satisfied.

Three Core Components:

1. Security Attacks

- **Definition**: Any action that compromises the security of information owned by an organization
- **Types**:
  - **Passive Attacks**: Traffic analysis, Release of message contents
  - **Active Attacks**: Masquerade, Replay, Modification of messages, Denial of Service

2. Security Services

- **Authentication Services**:
  - Peer Entity Authentication
  - Data Origin Authentication
- **Access Control**: Prevents unauthorized resource access
- **Confidentiality Services**:
  - Connection Confidentiality
  - Connectionless Confidentiality
  - Selective-field Confidentiality
  - Traffic Flow Confidentiality
- **Integrity Services**:
  - Connection Integrity (with/without recovery)
  - Connectionless Integrity
- **Non-repudiation Services**:
  - Origin Non-repudiation
  - Delivery Non-repudiation

3. Security Mechanisms

- **Specific Mechanisms**: Encipherment, Digital Signature, Access Control, Data Integrity, Authentication Exchange, Traffic Padding, Routing Control
- **Pervasive Mechanisms**: Event detection, Security audit trail, Security recovery

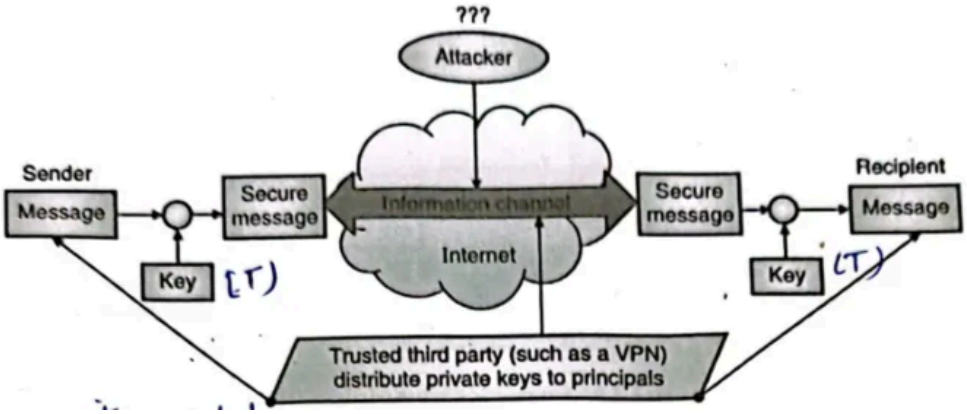
→ Network Security Model (NSM)

Definition: NSM is a seven-layer model that divides network security into manageable sections.

Seven NSM Layers:

1. **Physical Layer**: Safeguards physical network infrastructure
2. **VLAN Layer**: Network segmentation for controlled access
3. **ACL Layer**: Access Control Lists for network-layer filtering
4. **Software Layer**: Maintaining updated software with security patches
5. **User Layer**: User security training and awareness programs
6. **Administrative Layer**: Administrative staff training and security policies
7. **IT Department Layer**: Overall network security management

Key Principle: Each layer builds upon the previous layer; compromise of any layer affects all layers above it.



Q11. Steganography & Its Applications

Steganography:

- The art of hiding secret data within non-secret media (like images, audio, video, or text).
- Unlike cryptography, which hides the *content*, steganography hides the *existence* of the message.

Applications:

1. **Confidential communication**: Hide messages in images for secure transfer.
2. **Digital watermarking**: Protect intellectual property by embedding copyright info.
3. **Covert communication**: Used in intelligence or military for secret message passing.

4. **Data integrity checking**: Embedding checksums to verify tampering.

Q12. Explain Security Services & Mechanisms to Implement

Security services are advanced methods recommended to be offered at various OSI layers to ensure the security of systems and data transfer. According to X.800 and RFC 2828 standards, security services are communication services provided by a system to give protection to system resources.

Security Services & Mechanisms to Implement

→ Security Services

1. Authentication

- Peer entity authentication - verifies communicating parties are legitimate
- Data origin authentication - confirms data source authenticity

2. Access Control

- Controls and limits access to system resources
- Prevents unauthorized use of resources

3. Confidentiality

- Data confidentiality - protects data from unauthorized access
- Connection/connectionless confidentiality - protects transmitted data
- Traffic flow confidentiality - hides communication patterns

4. Integrity

- Connection integrity - detects data modification with/without recovery
- Connectionless integrity - ensures single data block integrity
- Prevents unauthorized data alteration

5. Non-Repudiation

- Origin non-repudiation - proof message was sent by specified party
- Destination non-repudiation - proof message was received

Security Mechanisms

Specific Security Mechanisms:

- **Encipherment** - Mathematical algorithms to transform data (encryption)
- **Digital Signature** - Cryptographic transformation for authenticity
- **Access Control** - Enforce access rights to resources
- **Data Integrity** - Mechanisms to ensure data hasn't been modified
- **Authentication Exchange** - Verify entity identity through information exchange

Pervasive Security Mechanisms:

- **Traffic Padding** - Insert bits to frustrate traffic analysis
- **Routing Control** - Select secure routes for data transmission
- **Event Detection** - Detect security-related events
- **Security Audit Trail** - Collect data for security auditing
- **Security Recovery** - Handle recovery from security breaches

These services work together to provide comprehensive network security by ensuring the CIA triad (Confidentiality, Integrity, Availability) and additional security properties.

Q13. Enlist Security Goals & Discuss Their Significance

Primary Security Goals (CIA Triad)

1. Confidentiality

- **Definition**: Ensures sensitive information is accessible only to authorized users
- **Significance**:
  - Protects privacy and trade secrets
  - Prevents competitive disadvantage
  - Complies with data protection regulations (GDPR)
- **Implementation**: Encryption, access controls, data classification
- **Risks**: Unauthorized access, weak encryption, insider threats

2. Integrity

- **Definition**: Maintains data accuracy and trustworthiness throughout its lifecycle
- **Significance**:
  - Ensures decision-making based on accurate data
  - Maintains system reliability and user trust
  - Critical for financial and medical systems
- **Implementation**: Hashing, checksums, version control, audit trails
- **Risks**: Data tampering, unauthorized modifications, system corruption

3. Availability

- **Definition**: Guarantees authorized users can access information when needed
- **Significance**:
  - Ensures business continuity and operations
  - Prevents revenue loss from system downtime

    - Maintains customer satisfaction and trust

- **Implementation**: Redundancy, backup systems, disaster recovery, load balancing
- **Risks**: DoS attacks, hardware failures, natural disasters

Extended Security Goals

4. Authentication

- **Significance**: Verifies entity identity before granting access
- **Applications**: Login systems, digital signatures, biometric verification

5. Non-repudiation

- **Significance**: Provides proof of actions for legal and audit purposes
- **Applications**: Digital contracts, financial transactions, email communications

6. Authorization

- **Significance**: Determines what authenticated entities can access
- **Applications**: Role-based access control, permission management

Q14. Explain Transposition Ciphers with Illustrative Examples

Definition
Transposition ciphers rearrange plaintext characters according to a system without altering the characters themselves. Only the **positions change**, not the symbols.

Types of Transposition Ciphers

1. Keyless Transposition (Rail Fence Cipher)

Write plaintext in zigzag pattern, read row-wise.

Example: Encrypt "**SAVE THE KING**" using 3 rails

```
Rail 1: S   t   i
Rail 2: a e h k n g
Rail 3: V   e
```

Ciphertext: "**STIAEKHNGVE**"

2. Keyed Transposition (Columnar Cipher)

Arrange plaintext under keyword, rearrange columns alphabetically.

Example: Encrypt "**ATTACK AT ONCE**" with key "**ZEBRA**"

Step 1: Arrange under key

```
textZ E B R A
5 2 1 4 3
A T T A C
K A T O N
C E X X X
```

Step 2: Read columns in alphabetical order (A=3, B=1, E=2, R=4, Z=5)

- B(1): **TTX**
- E(2): **TAE**
- A(3): **COX**
- R(4): **AOX**
- Z(5): **AKC**

Ciphertext: "**TTXTAECOXAOXAKC**"

Advantages: Simple, preserves character frequency

Disadvantages: Vulnerable to pattern analysis, limited key space, susceptible to known plaintext attacks

Transposition ciphers form the basis for diffusion in modern cryptography

Q15. Distinguish Between Active and Passive Security Attacks

Attribute	Active Attack	Passive Attack
Complexity	High	Low
Impact	High	Low
Detection Possibility	High	Low
Prevention Possibility	Low	High
Duration	Short	Long
System Behavior	Modified	Unaffected
Original Information	Modified	Unaffected
Purpose	Harm ecosystem	Learn about ecosystem

Q16. What are Block Cipher Modes. Describe Any Two Block Cipher Modes in Detail

For this answer, you can refer

1. Electronic Codebook (ECB) Mode

Algorithm Description:

- **Encryption**: Each plaintext block encrypted independently
- **Formula**: Cj = E_K(Pj) for j = 1...n
- **Decryption**: Pj = D_K(Cj) for j = 1...n

Characteristics:

- Simplest block cipher mode
- Each block treated independently
- Same plaintext block → same ciphertext block

- Suitable for single-block messages only

Advantages:

- **Parallel Processing**: Encryption and decryption can be parallelized
- **Simple Implementation**: Straightforward to code and understand
- **Error Localization**: Errors in one block don't affect others
- **Random Access**: Any block can be decrypted independently

Disadvantages:

- **Pattern Leakage**: Identical plaintext blocks produce identical ciphertext
- **Statistical Analysis**: Frequency analysis possible on large datasets
- **Security Weakness**: Not suitable for multi-block messages
- **Predictability**: Attacker can identify repeated patterns

Security Issues:

- **Known Plaintext Attack**: If attacker knows some plaintext-ciphertext pairs
- **Chosen Plaintext Attack**: Attacker can build codebook of encryptions
- **Pattern Analysis**: Images encrypted with ECB show visible patterns

2. Cipher Block Chaining (CBC) Mode

Algorithm Description:

- **Encryption**: C0 = IV, Ci = E_K(Pi $\oplus$ Ci-1) for i = 1...n
- **Decryption**: Pi = D_K(Ci) $\oplus$ Ci-1 for i = 1...n
- **Initialization Vector (IV)**: Unique, unpredictable value for each encryption

Characteristics:

- Each plaintext block XORed with previous ciphertext before encryption
- First block uses Initialization Vector (IV)
- Chaining makes each ciphertext block dependent on all previous blocks
- Same plaintext encrypted differently each time (due to IV)

Advantages:

- **Pattern Hiding**: Identical plaintext blocks produce different ciphertext
- **Semantic Security**: Same plaintext produces different ciphertext with different IVs
- **Parallel Decryption**: Decryption can be parallelized (encryption cannot)
- **Error Propagation Control**: Errors affect only current and next block

Disadvantages:

- **Sequential Encryption**: Must encrypt blocks in sequence

- **IV Management**: Requires secure IV generation and transmission
- **Padding Attacks**: Vulnerable to padding oracle attacks if improperly implemented
- **Error Propagation**: Single bit error affects current and next block

Security Features:

- **IV Requirements**: Must be unpredictable and unique per encryption
- **Semantic Security**: Provides probabilistic encryption
- **CPA Security**: Secure against chosen-plaintext attacks with proper IV

Implementation Considerations:

- **IV Transmission**: IV can be transmitted openly (not secret)
- **Padding**: Last block requires padding if not full block size
- **Performance**: Slightly slower than ECB due to chaining dependency

Q17. Given modulus n = 221 & public key e = 7. Find the values of p, q, phi(n) and d using RSA. Encrypt M = 5

Given: n = 221, e = 7, M = 5

Step 1: Find Prime Factors of n = 221

I need to factorize 221:
221 = 13 × 17
Therefore: **p = 13, q = 17**

Step 2: Calculate φ(n)

φ(n) = (p-1)(q-1) = (13-1)(17-1) = 12 × 16 = **192**

Step 3: Find Private Key d

d must satisfy: (e × d) mod φ(n) = 1

(7 × d) mod 192 = 1

Using **Extended Euclidean Algorithm** to find multiplicative inverse of 7 mod 192:

Index i	quotient q	Remainder r	s	t
0		192	1	0
1		7	0	1
2	27	3	1	-27
3	2	1	-2	55
4	3	0	-	-

From the table: x = 55, y = -2

Verification: 7 × 55 + 192 × (-2) = 385 - 384 = 1 ✓

Therefore: **d = 55**

Step 4: Encryption

C = M^e mod n = 5^7 mod 221

Calculating 5^7 mod 221:

- 5^1 = 5
- 5^2 = 25
- 5^4 = 625 mod 221 = 183

5^7 = 5^4 × 5^2 × 5^1 = 183 × 25 × 5 mod 221

- 183 × 25 = 4575 mod 221 = 155
- 155 × 5 = 775 mod 221 = 112

Therefore: **C = 112**

Step 5: Verification (Decryption)

M = C^d mod n = 112^55 mod 221 = 5 ✓

Final Answer:

- **Prime factors:** p = 13, q = 17
- **φ(n) = 192**
- **Private key:** d = 55
- **Public key:** (e, n) = (7, 221)
- **Private key:** (d, n) = (55, 221)
- **Encrypted message:** C = 112

The message M = 5 is successfully encrypted to ciphertext C = 112 using the RSA algorithm.

Q18. Explain the CIA triad (5 marks)

The CIA Triad

The **CIA triad** represents the three fundamental pillars or tenets of information security. CIA stands for **Confidentiality, Integrity, and Availability** - these are the core security principles that form the foundation of any secure information system.

1. Confidentiality
Confidentiality ensures that information is kept secret and is accessible only to authorized entities.

Key aspects:

- Protects information from unauthorized disclosure
- Information should be protected at **rest** (when stored), in **motion** (during transmission), and during **use** (when processing)

- Only intended recipients should be able to access the contents of a message

Mechanisms used:

- Encryption
- Access control
- Data classification

Example: Using encryption when sending confidential emails or protecting PIN numbers during ATM transactions.

2. Integrity
Integrity ensures that information remains intact and is not modified by unauthorized entities.

Key aspects:

- Protects information from unauthorized modification, addition, or deletion
- Ensures data received is exactly as sent by authorized entity
- Any modification should only be done by authorized persons through authorized mechanisms

Types:

- **Data Integrity**: Information is changed only in authorized manner
- **System Integrity**: System performs intended functions without unauthorized manipulation

Mechanisms used:

- Hashing
- Access control
- Input/output sanitization

Example: Email integrity - ensuring the email you receive hasn't been altered during transmission.

3. Availability
Availability ensures that information and system resources are accessible and usable when needed by authorized users.

Key aspects:

- Resources must be available to authorized users at all times when required
- Protects against unauthorized destruction or denial of access
- Extends to equipment like computers, network devices, and printers

Mechanisms used:

- Access control
- Backup systems
- Disaster recovery processes
- Business continuity planning

Example: Bank systems being available 24/7 for customer transactions, or log files being available for system monitoring.

Q19: Given a 5×5 grid and the keyword "PLAYFAIR", encrypt the message "HIDE" using the Playfair cipher. Demonstrate the steps & the final ciphertext (5 marks)

Step 1: Construct the 5×5 Key Matrix

Using keyword "PLAYFAIR":

- Remove duplicate letters: P-L-A-Y-F-A-I-R → P-L-A-Y-F-I-R (remove second A)
- Fill 5×5 matrix with keyword first, then remaining letters alphabetically (I/J combined):

```
P L A Y F
I R B C D
E G H K M
N O Q S T
U V W X Z
```

Step 2: Prepare the Plaintext

Message: "HIDE"

- Group into pairs: "HI", "DE"
- No repeated letters in pairs, even length - no changes needed

Step 3: Apply Playfair Rules

For pair "HI":

- H is at position (row 2, column 2)
- I is at position (row 1, column 0)
- Since they're in different rows AND different columns → **Rectangle Rule**
- H maps to same row (2), column of I (0) → **E**
- I maps to same row (1), column of H (2) → **B**
- "HI" → "EB"

For pair "DE":

- D is at position (row 1, column 4)
- E is at position (row 2, column 0)
- Since they're in different rows AND different columns → **Rectangle Rule**
- D maps to same row (1), column of E (0) → **I**
- E maps to same row (2), column of D (4) → **M**
- "DE" → "IM"

Step 4: Final Result

Original message: "HIDE"

Encrypted message: "EBIM"

Answer: The ciphertext is "EBIM"