Cryptography and Network Security – Assignment Answer Key

# 1. OSI Security Architecture

Definition: OSI security architecture provides a layered approach to network security with services like confidentiality, integrity, and authentication.

Attacks: Passive (e.g., eavesdropping) and Active (e.g., modification).

Mechanisms: Encipherment, digital signatures, access control.

Services: Authentication, confidentiality, data integrity, non-repudiation.

# 2. Active vs Passive Attack

Active: Alters data (e.g., DoS).

Passive: Just observes (e.g., traffic analysis).

Passive is harder to detect, active easier to notice.

# 3. AES Encryption Process

Steps: SubBytes → ShiftRows → MixColumns → AddRoundKey.

Works on 128-bit blocks using S-box and matrix operations.

# 4. Playfair Cipher Encryption

Keyword: MONARCHY, Plaintext: 'swaraj is my birth right'.

Pairs with 'X' filler: SW, AR, AJ, IS...

Encrypted Text: TXRORKTHBHGKTRTHKCUG.

# 5. DES Algorithm

Symmetric 64-bit block cipher using 56-bit key.

16 Feistel rounds: Expansion, Substitution (S-box), Permutation.

Vulnerable to brute-force.

# 6. RSA Encryption

Given: p=7, q=11, e=17, m=8 → n=77, φ(n)=60.

d=53. Ciphertext = 8^17 mod 77 = 57, Decrypted = 57^53 mod 77 = 8.

# 7. String vs Block Cipher

String: Bit-by-bit (e.g., RC4).

Block: Fixed-size blocks (e.g., AES, DES).

# 8. CIA Triad

Confidentiality: Prevent unauthorized access.

Integrity: Prevent unauthorized modification.

Availability: Ensure access to data/services.

# 9. Symmetric Cipher Techniques

Uses single key for encryption/decryption.

Substitution (Caesar, Playfair) and Transposition (Rail Fence).

# 10. ECB Mode

Encrypts each block independently.

Fast but leaks patterns in repeated blocks.

# 11. Symmetric vs Asymmetric Key

Symmetric: Same key, faster.

Asymmetric: Public/private key pair, more secure.

# 12. X.800 Security Services

Authentication, Access Control, Confidentiality, Integrity, Non-repudiation.

# 13. Rail Fence Cipher Example

Plaintext: 'WEAREDISCOVEREDRUNATONCE'.

Key = 3 → Ciphertext: WECRUOERDSOEENATNAIVDRRE.

# 14. MITM Attack

Attacker intercepts communication (e.g., over public Wi-Fi).

Countermeasures: HTTPS, VPNs, SSL.

# 15. Steganography

Hiding messages in media (e.g., images, audio).

Unlike cryptography, it hides existence, not meaning.

# 16. Computer Security Objectives

CIA: Confidentiality, Integrity, Availability.

Includes authentication and access control.

# 17. Substitution vs Transposition

Substitution: Change characters (e.g., Caesar).

Transposition: Change order (e.g., Rail Fence).

# 18. Rail Fence Cipher (Key = 4)

Plaintext: 'theyareattackingfromthenorth'.

Ciphertext: TAKOTHRTANHHHEETCGERRYAIMT.

# 19. Cryptanalysis vs Brute Force

Cryptanalysis: Logical attack based on cipher weaknesses.

Brute Force: Tries every key combination until success.

# 20. Caesar Cipher (Key = 3)

Plaintext: 'hidethegoldanddefendeastwall'.

Ciphertext: klghwkhjrogdqgghihhqdghdvwzdoo.