Type: MCQ

Q1. Name the security mechanism where a trusted 3rd party is used to assure certain properties of a data exchange (0.5)

1. **Notarization
2. Confidentiality
3. Authorization
4. Authentication

Q2. In which of the modes of block cipher, each block of 64 plaintext bits is encoded independently using the same key? (0.5)

1. **Electronic Codebook (ECB) mode
2. Cipher Block Chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)

Q3. Given the cipher text: "**LEROPxEMCTAxCTYGHxWOOPRY**". Written in blocks of five and key as "**tech**" Decrypt the cipher text to get the plain text using keyed transposition cipher (Keyword Columnar Transposition). [Padding character used here is x]. (0.5)

1. CryptographyXXXWelcome
2. **Welcometocryptographyxxx
3. WelcomeXXXCryptography
4. WelcomeXtoXcryptographyxxx

Q4. An attacker sends an encrypted message to a server using RSA, where the server is using the public key e=3. The attacker notices that if the message is too small, the ciphertext is simply the cube of the message. The attacker uses this property to easily recover the original message without needing to decrypt it. What type of attack is this? (0.5)

1. Chosen-ciphertext attack
2. Timing attack
3. **Low-exponent attack
4. Factoring attack

Q5. Alice and Bob agree on a prime number p=11 and a primitive root g=2. Alice chooses her private key a=4, and Bob chooses his private key b=3. They exchange their public keys. What is the shared secret key they both compute? (0.5)

1. 2
2. 5
3. **4

4. 8

Q6. Which method is commonly used to verify the integrity of a message in cryptographic communication? (0.5)

1. **Message digest generated by SHA-256
2. AES Symmetric encryption algorithms
3. Digital certificates signed by a certificate authority
4. Elliptic curve cryptography

Q7. Which statement about Data Encryption Standard is accurate? (0.5)

1. It has a fixed block size but allows for dynamic key lengths
2. **It shows a strong avalanche effect
3. It uses 56-bit keys, making it immune to brute force attacks
4. It lacks diffusion, making it vulnerable to frequency analysis

Q8. Consider a public-key encryption system with a 2048-bit key. How many possible keys exist for this system? (0.5)

1. 2^(2^2048)
2. **2^2048
3. 2048^2
4. 2^1024 mod 2048

Q9. How does a polyalphabetic substitution cipher improve security over a simple substitution cipher? (0.5)

1. By using multiple keys
2. **By changing the substitution pattern for each letter
3. By increasing the block size and adding noise
4. By using a different algorithm

Q10.The security of the ElGamal cryptosystem relies on the difficulty of solving which of the following problems? (0.5)

1. **Discrete Logarithm Problem
2. Integer Factorization Problem
3. Elliptic Curve Problem
4. Shortest Path Problem

Type: DES

11	Using the ElGamal encryption scheme with the parameters p=13, e_1=2, r=5 and d=3, show how Bob proves that the message has indeed come from Alice by following these steps: **Solution:** p = 13, e_1 = 2, d = 3, **$e_2 = 2^3 \bmod 13 = 8$** Public key: {p, e_1, e_2 } = {13, 2, 8} **i) How does Alice select the value of r? [0.5]** The random value r is selected as a random integer between 1 and *p−2*, ensuring it is co-prime with *p−1*. **ii) Encrypt the message "11". [1.5 Marks]** **Encryption:** $C_1 = e_1^r \bmod p = 2^5 \bmod 13 = 6$ $C_2 = (M * e_2^r) \bmod p = 11 * 8^5 \bmod 13 = 10$ **Cipher text: (6, 10)** **iii) Decrypt the ciphertext to retrieve the original message. [1Marks]** **Decryption :** $[C_2 * (C_1^d)^{-1}] \bmod p = = 10 * (6^3)^{-1} \bmod 13 =$ **11** **IV. If Alice uses Random value r=352 and encrypts the same message, is Bob able to decrypt the message? Justify your answer. [1 Marks]** **If Alice uses Random value r=352,** p = 13, e_1 = 2, d = 3, $e_2 = 2^3 \bmod 13 = 8$ **C1=1** **C2=11** $[C_2 * (C_1^d)^{-1}] \bmod p = = 11 * (1^3)^{-1} \bmod 13 = 11$ Yes, Bob will be able to compute plain text as r can be any random integer chosen by Alice. Yes, it is possible to use *r=352* because the ElGamal encryption algorithm reduces *r mod (p−1)*. In this case, *352mod 12=4*, so using *r=352* is equivalent to using *r=4* for the encryption process. This reduction ensures that Bob can still decrypt the message correctly and recover *m=11*.

12

Given the hex code of the plaintext {00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F} and the initial key {24 75 A2 B3 34 75 56 88 31 E2 12 00 13 AA 54 87} answer the following by applying the functions of Advanced Encryption Standard. Refer to the tables 12 (a) and 12 (b).

a. Show the value of the State after SubBytes.

b. Show the value of the State after ShiftRows.

c. Using Key Expansion method compute W_4 for the initial key stream given above.

Table 12 (a) : RCON Constants

Round	*Constant (RCon)*	*Round*	*Constant (RCon)*
1	$(\underline{\mathbf{01}}\ 00\ 00\ 00)_{16}$	6	$(\underline{\mathbf{20}}\ 00\ 00\ 00)_{16}$
2	$(\underline{\mathbf{02}}\ 00\ 00\ 00)_{16}$	7	$(\underline{\mathbf{40}}\ 00\ 00\ 00)_{16}$
3	$(\underline{\mathbf{04}}\ 00\ 00\ 00)_{16}$	8	$(\underline{\mathbf{80}}\ 00\ 00\ 00)_{16}$
4	$(\underline{\mathbf{08}}\ 00\ 00\ 00)_{16}$	9	$(\underline{\mathbf{1B}}\ 00\ 00\ 00)_{16}$
5	$(\underline{\mathbf{10}}\ 00\ 00\ 00)_{16}$	10	$(\underline{\mathbf{36}}\ 00\ 00\ 00)_{16}$

Table 12 (b) : Sub Bytes

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Scheme 12

i. STATE

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

ii.

63	**F2**	**30**	**FE**
7C	**6B**	**01**	**D7**
77	**6F**	**67**	**AB**
7B	**C5**	**2B**	**76**

SUBYTES

63	**F2**	**30**	**FE**
6B	**01**	**D7**	**7C**
67	**AB**	**77**	**6F**
76	**7B**	**C5**	**2B**

iii. SHIFTROWS

iv. KEY EXPANSION

W_0[24 75 A2 B3] W_1[34 75 56 88] W_2[31 E2 12 00] W_3[13 AA 54 87]

$(i \bmod 4) \neq 0, w_i = w_{i-1} \oplus w_{i-4}$.

W_4=8955B5CE

$(i \bmod 4) = 0, w_i = t \oplus w_{i-4}$. Here t, a temporary word.

$t = \text{SubWord}(\text{RotWord}(w_{i-1})) \oplus \text{RCon}_{i/4}$

RotWord (13AA5487) = AA548713 → **SubWord** (AA548713) = AC20177D

t = AC20177D ⊕ **RCon**$_1$ = AC20 17 7D ⊕ 01000000_{16} = AD20177D

Each Part 1 M

13 With respect to Data Encryption Standard (DES), answer the following questions

a. What is the purpose of S-Box in DES?

b. Explain in brief the different types of Weak Keys in DES.

c. DES is resilient to Avalanche and Completeness effect. Then why is Double DES prevalent? Also, name and illustrate the attack which double DES cannot withstand.

	### a. Purpose of S-Box in DES The S-Box (Substitution Box) in DES (Data Encryption Standard) plays a crucial role in the encryption process by introducing non-linearity and complexity, making the cipher more resistant to cryptanalysis. Specifically, it: 1. **Provides Confusion**: By transforming the input bits into different output bits, S-Boxes create confusion, which obscures the relationship between the ciphertext and the plaintext, making it difficult for attackers to deduce the original message. 2. **Non-linearity**: The S-Boxes replace 6-bit inputs with 4-bit outputs according to a predefined table, ensuring that small changes in the input lead to significant changes in the output. This non-linear transformation contributes to the avalanche effect, where a small change in the input (such as flipping a single bit) results in a substantial change in the output. 3. **Security**: They are designed to maximize security by preventing simple linear and differential cryptanalysis, providing resistance against certain attacks that exploit the linearity in cryptographic systems. ### b. Different Types of Weak Keys in DES Weak keys in DES are specific keys that, due to the structure of DES, can result in undesirable properties such as encryption and decryption being the same operation. There are four types of weak keys: 1. **Weak Keys**: These are keys where the encryption and decryption operations are identical, meaning `E_k(E_k(x)) = x`. There are four weak keys in DES, characterized by patterns like all zeros or all ones in subkeys. - Examples: `0000000000000000` (all 0s) and `FFFFFFFFFFFFFFFF` (all 1s). 2. **Semi-Weak Keys**: There are 12 semi-weak key pairs. In these cases, two different keys exist such that encryption with one key and then decryption with the other key results in the original plaintext. - Examples: `(0101010101010101, FEFEFEFEFEFEFEFE)` and their pairwise complements.

3. **Possible Weak Keys**: These keys have patterns where specific subkeys repeat throughout the DES rounds, reducing the complexity of the encryption process.

- These are not as problematic as weak or semi-weak keys but still pose a reduced level of security.

4. **Complementary Keys**: For any given DES key `K`, the complementary key is `K'` where each bit is the complement of the corresponding bit in `K`. The ciphertext `C` produced by encrypting a plaintext `P` with `K` and `K'` are related by complementing `C`.

- Property: `E_K(P) = C` and `E_(K')(P) = C'`.

c. Double DES and the Attack It Cannot Withstand

Double DES: Double DES involves applying DES encryption twice with two different keys (K1 and K2), resulting in an effective key length of 112 bits (2 × 56 bits). It was introduced to increase the key space and hence improve the security over single DES, which has only a 56-bit key space.

Why Double DES is Prevalent:

- **Increased Key Space**: It offers a larger key space compared to single DES, which theoretically makes brute-force attacks more difficult.

- **Defense against Certain Attacks**: It offers better resistance against attacks that are effective on single DES, though it is still vulnerable to specific attacks (described below).

Attack Double DES Cannot Withstand:

- **Meet-in-the-Middle Attack**: This is an efficient attack against double DES that reduces its effective security. The attack works as follows:

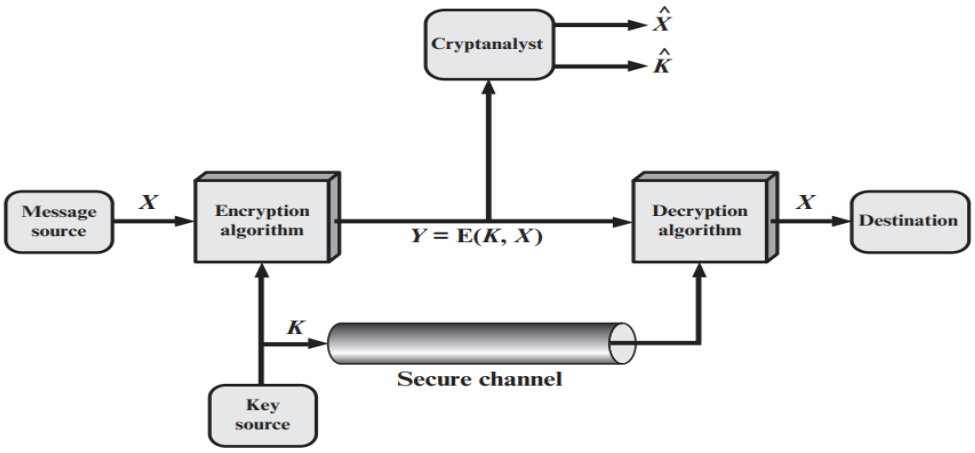
1. **Encrypt** the plaintext `P` with all possible keys `K1` to generate intermediate ciphertexts.

2. **Decrypt** the ciphertext `C` with all possible keys `K2` to generate another set of intermediate plaintexts.

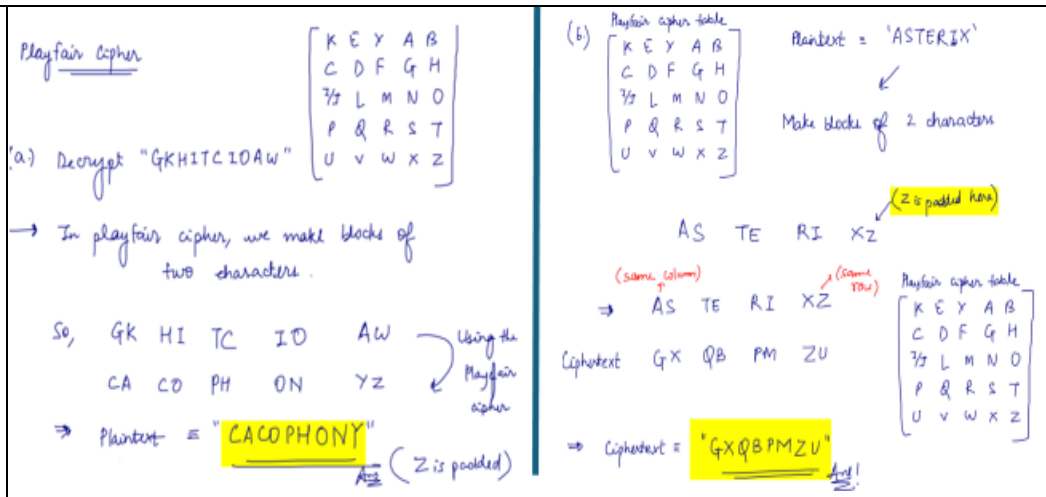
	3. **Compare** the two intermediate values to find a match. When a match is found, the corresponding `K1` and `K2` are considered as candidate keys. The meet-in-the-middle attack effectively reduces the complexity from `2^112` (brute force attack on double DES) to `2^56 + 2^56` (due to the need to store intermediate results), making double DES only slightly more secure than single DES. ### Illustration of the Meet-in-the-Middle Attack: 1. **Step 1**: Encrypt plaintext `P` with all `2^56` possible values of `K1` to get intermediate values `I`. 2. **Step 2**: Decrypt ciphertext `C` with all `2^56` possible values of `K2` to get intermediate values `J`. 3. **Step 3**: Look for matches between `I` and `J`. The matched pair (`K1`, `K2`) is the key. This attack's efficiency is why Triple DES (3DES), which uses three DES operations with either two or three keys, is often preferred over double DES, providing better security against such attacks. **Each Part 1 M**
14	Using the Rabin cryptosystem with p = 47 and q = 11. If the cipher text C, generated for a plain text P is 289, find the possible answers for P. **Ans: [Finding roots: 1M; Apply Chinese reminder: 2M]** We first find n = p × q = 47 × 11 = 517. $a_1 = +C^{(p+1)/4} \bmod p = +289^{12} \bmod 47 = +17$ and $a_2 = -17 \Rightarrow 30$. $b_1 = +C^{(q+1)/4} \bmod q = +289^{3} \bmod 11 = +5$ and $b_2 = -5 \Rightarrow 6$. Now, we have four pairs of solutions for a1, a2 and b1, b2: 1. $x \equiv 17 \pmod{47}$ and $x \equiv 5 \pmod{11}$ 2. $x \equiv 17 \pmod{47}$ and $x \equiv 6 \pmod{11}$ 3. $x \equiv 30 \pmod{47}$ and $x \equiv 5 \pmod{11}$ 4. $x \equiv 30 \pmod{47}$ and $x \equiv 6 \pmod{11}$ We will solve these congruences using the Chinese Remainder Theorem. **$x \equiv 17 \pmod{47}$ and $x \equiv 5 \pmod{11}$** We solve this system using the method of successive substitution: $x = 47k + 17$.

	47k + 17 ≡ 5 (mod 11). Reduce 47 mod 11, giving us 47 ≡ 3 (mod 11). Now, 3k + 17 ≡ 5 (mod 11) => 3k ≡ -12 (mod 11). Simplify: -12 ≡ -12 + 11 = -1 ≡ 10 (mod 11). We now have 3k ≡ 10 (mod 11). To solve this, multiply both sides by the inverse of 3 modulo 11, which is 4 (since 3 × 4 ≡ 1 (mod 11)). Multiply: k ≡ 40 (mod 11) => k ≡ 7 (mod 11). Substitute k = 7 back into x = 47k + 17: x = 47(7) + 17 = 346. Thus, the solution is x ≡ 346 (mod 517). **x ≡ 17 (mod 47) and x ≡ 6 (mod 11)** x = 47k + 17. Substitute into the second congruence: 47k + 17 ≡ 6 (mod 11). 3k + 17 ≡ 6 (mod 11) => 3k ≡ -11 ≡ 0 (mod 11). So, k ≡ 0 (mod 11). Substitute k = 0 into x = 47k + 17: x = 47(0) + 17 = 17. Thus, the solution is x ≡ 17 (mod 517). **x ≡ 30 (mod 47) and x ≡ 5 (mod 11)** Start with x = 47k + 30. Substitute into the second congruence: 47k + 30 ≡ 5 (mod 11). Reduce 47 mod 11, giving us 47 ≡ 3 (mod 11). Now, 3k + 30 ≡ 5 (mod 11) => 3k ≡ -25 ≡ 8 (mod 11). We now have 3k ≡ 8 (mod 11). Multiply both sides by the inverse of 3 modulo 11, which is 4. Multiply: k ≡ 32 (mod 11) => k ≡ 10 (mod 11). Substitute k = 10 back into x = 47k + 30: x = 47(10) + 30 = 500. Thus, the solution is x ≡ 500 (mod 517). **x ≡ 30 (mod 47) and x ≡ 6 (mod 11)** x = 47k + 30. Substitute into the second congruence: 47k + 30 ≡ 6 (mod 11).

	3k + 30 ≡ 6 (mod 11) => 3k ≡ -24 ≡ 9 (mod 11). We now have 3k ≡ 9 (mod 11). Multiply both sides by the inverse of 3 modulo 11, which is 4. Multiply: k ≡ 36 (mod 11) => k ≡ 3 (mod 11). Substitute k = 3 back into x = 47k + 30: x = 47(3) + 30 = 171. Thus, the solution is x ≡ 171 (mod 517). The four possible plaintexts P that correspond to the ciphertext C = 289 are: P = 346, 17, 500, 171.
15	Briefly outline the three key criteria for evaluating cryptographic hash functions with an attack associated with each that reveals how failing the criterion compromises security. Scheme: **3 X1M each for** **- 0.5M Identification of criterion + Brief math explanation of the criterion** **- 0.5M Attack associated with Criterion and how failing this criterion compromises security** **Expected Answer:** **1. Preimage Resistance:** It should be computationally infeasible to find the original input x given only the hash output h(x) **0.5M** **Attack**: If an attacker can reverse a hash and find the original message from the hash output, they can break confidentiality or authenticity. For instance, if a password hash is reversed, the attacker can retrieve the password. **0.5M** **2. Second Preimage Resistance**: Given an input x1, it should be computationally infeasible to find a different input x2 such that h(x1)=h(x2) (i.e., two inputs with the same hash). **0.5M** **Attack**: If an attacker can find a second input with the same hash, they can substitute one valid message for another without detection. This can compromise integrity, for example, altering a digital signature without invalidating it. **0.5M** **3. Collision Resistance:** It should be computationally infeasible to find any two different inputs x1 and x2 such that h(x1)=h(x2). **0.5M**

	Attack: If an attacker can find two different inputs that produce the same hash, they can create fraudulent transactions or messages with the same hash as valid ones, leading to security breaches such as in digital certificates or contracts. **0.5M**
16	Given a scenario, with the help of the model diagram where sensitive data must be transmitted securely over a public network, design a cryptographic system that incorporates symmetric encryption. Justify your choices and do the crypt analysis. Answer: Following Diagram must be drawn or at least the architectural diagram of the chosen choice must be drawn. As the sensitivity of the data is high, the selected choice must not be susceptible to very well know cyber-attacks. If the selected choice is not strong enough, the grade will be accordingly awarded (this shows the applicability of the concepts in the real-world scenario). Diagram and explanation carry **1.5 Marks.** The selected choice must be justified, and it carries **0.5 Marks.** Cryptanalysis of the choice carries **1 Marks**.  Figure 3.2 Model of Symmetric Cryptosystem
17	Define Elliptic Curves over Real numbers. What are the properties of operation in ECC? **Ans:** [Definition: 0.5M; Properties: 1.5M] An elliptic curve is defined by an equation in two variables with coefficients. For cryptography, the variables and coefficients are restricted to elements in a finite field, which results in the definition of a finite abelian group. Elliptic curves are not ellipses. They are so named because they are described by cubic equations, like those used for calculating an ellipse's circumference. In general, cubic equations for elliptic curves take the following form, known as a Weierstrass equation: y2 = x3 + ax + b

	Properties of the Operation The following are brief definitions of the properties of the operation: 1. Closure: It can be proven that adding two points, using the addition operation defined in the previous section, creates another point on the curve. 2. Associativity: It can be proven that (P + Q) + R = P + (Q + R). 3. Commutativity: The group made from the points on a non-singular elliptic curve is an abelian group; it can be proven that P + Q = Q + P. 4. Existence of identity: The additive identity in this case is the zero point, O. In other words P = P + O = O + P. 5. Existence of inverse: Each point on the curve has an inverse. The inverse of a point is its reflection with respect to the x-axis. In other words, the point P = (x1, y1) and Q = (x1, −y1) are inverses of each other, which means that P + Q = O. Note that the identity element is the inverse of itself.
18	You are a secret agent tasked with decoding a mysterious message intercepted from an enemy communication. Using the Playfair cipher given below a. Decrypt the encoded message 'GKHITCIOAW' to reveal its hidden contents. b. You need to send a secure message to your allies. Encrypt the plaintext 'ASTERIX' using the same cipher to ensure your message remains confidential.  Scheme: 2 X 1M for all letter pairs encoded/decoded correctly, including padding, no partial marking for encryption or decryption. Solution:

	 a.1M awarded If Decoding of 'GKHITCIOAW' is • shown pairwise in steps AND • the answer is completely correct 'CACOPHONY' AND • Answer is finally indicated as a one word Plaintext. b.1M awarded If Encoding of 'ASTERIX' is • shown pairwise in steps with padding letter explicitly indicated AND • the answer is completely correct 'GXQBPMZZ' (last letter may change if padding is other than X AND • Answer is finally indicated as a one word CipherText.
19	Differentiate security services and security mechanisms. Analyse the relationship between them and give an example. **Answer:** Differentiation carries **1 Marks** Analysis of Relationship between them carries **0.5 Marks** Examples carries **0.5 Marks** Security services and security mechanisms are interconnected concepts in information security aimed at protecting data and systems from unauthorized access, attacks, and other threats. However, they serve distinct roles. **Security Services** **Definition:** Security services are the functions or capabilities to enhance the security of data processing systems and information transfers.

	Purpose: They address specific security needs and goals, such as confidentiality, integrity, availability, and non-repudiation. Examples: **Confidentiality:** Ensuring that data is accessible only to authorized individuals. Integrity: Protecting data from unauthorized modification or destruction. **Availability:** Ensuring that data and systems are accessible when needed. Non-repudiation: Preventing one party from denying involvement in a transaction or communication. **Security Mechanisms** **Definition:** Security mechanisms are the techniques, technologies, or procedures to implement security services. **Purpose:** They provide the means to achieve the desired security objectives. Examples: Cryptography: Using mathematical algorithms to encrypt and decrypt data. Access controls: Limiting access to data and systems based on user identity and permissions. Firewalls: Filtering network traffic to block unauthorized access. Intrusion detection systems (IDS): Monitoring network traffic for signs of malicious activity. Relationship Between Services and Mechanisms Complementary: Security services and mechanisms are interdependent. Security services define the desired outcome, while security mechanisms provide the means to achieve it. **Multiple Mechanisms per Service:** A single security service can often be implemented using various mechanisms. For example, confidentiality can be achieved through encryption, access controls, and physical security measures. **Multiple Services per Mechanism:** A single security mechanism can contribute to numerous security services. For example, encryption can provide confidentiality, integrity, and non-repudiation.