PYQ

2021

1 (a) What is cryptography?

⇒ Cryptography is ~~a technique for~~ the practice and study of techniques for secure communication by transforming plaintext (readable data) into ciphertext (unreadable data) to protect it from unauthorized access.

(b) What is cipher?

⇒ A cipher is an algorithm that transforms plaintext (readable data) into cipher text (unreadable data) to protect it from unauthorized access.

(c) What is attack?

⇒ An attack refers to an attempt to compromise the security of a system, network, or data.

(d) What is Steganography?

⇒ Steganography is the practice of hiding secret information within a non-secret message, image, or other medium in such a way that the very existence of the secret information is not apparent

(e) What is watermarking?

⇒ watermarking is the process of embedding a hidden pattern or information, called a watermark, into a digital medium, such as an image, audio, or video file.

(f) what is threat?

→ Any potential occurrence that could compromise the security, integrity, or availability of an organization's assets, data, or systems.

(g) what is traffic padding?

→ Traffic padding is a technique used to conceal the true nature and pattern of network traffic by adding dummy or random data to the transmission.

(h) Define block cipher.

→ A block cipher is a type of symmetric-key encryption algorithm that:

1. Divides plaintext into fixed length blocks: Typically 64 to 128 bits
2. Encryption each block independently: using a shared secret key.
3. Produces a corresponding ciphertext block: of same length as the plaintext block.

2022

(1) (a) write a difference between cryptography and steganography.

→ cryptography: It encrypts data to convert it to a un readable form.

Steganography: It hides the data within another medium.

(b) What is meant by decryption?

→ Decryption is the process of converting encrypted data (ciphertext) back into its original, readable form (plaintext).

(c) ~~what is the~~ write a difference between virus and worm.

→ Virus: Requires a host program or file to replicate and spread.

Worm: can replicate and spread independently without a host program.

(d) What do you mean by Hacking?

→ Hacking refers to the unauthorized access, use, disclose, disruption, modification, or distruction of computer systems, networks, or electronic data.

(e) Define digital signature.

→ A digital signature is a cryptographic mechanism that:

1. varifies authentiety: confirms the identity of a sender or signer.
2. Ensures Integrity: Guarantees that the message or document has not been tampered with or altered.
3. Provide non-repudiation: Prevents the sender or signer from denying their involvement.

(f) what is Brute force Attack?

→ A brute force attack is a type of cyber attack where an attacker attempts to guess or crack a password, encryption key, or other sensitive information by trying all the possible combinations. and to do that they sometimes use automated tools.

(g) what is residual risk?

→ Residual risk is the remaining risk or threat that still exists after:

1. Implementing security controls.
2. Taking risk-reducing measures.

(h) what is proxy firewall?

→ A proxy firewall is a type of firewall that

1. Acts as an intermediary: Sits between a trusted network and an untrusted network (e.g., the internet).
2. Intercepts and filters traffic: Inspects and controls incoming and outgoing network traffic.
3. Hides internal network details: Conceals the IP addresses and other details of the internal network.

2022-23

(1) (a) what is Steganography?

(b) what do you mean by impersonation attack?

⇒ An impersonation attack is a type of cyber attack where an attacker:

1. Pretends to be someone else: Assumes the identity of a legitimate user, device, or system.
2. Mimic the victim's characteristics: ~~Imitates~~ Imitates the victim's behavior, credentials, or attributes to deceive others.

(c) what is watermarking?

(d) what is the main difference between substitution cipher and transposition cipher?

⇒ Substitution: Replaces each plaintext symbol (e.g. letter or digit) with a different symbol.

Transposition: Rearranges the plaintext symbols according to a specific pattern or algorithm.

(e) what is traffic padding?

(f) what do you mean by product cipher?

⇒ A product cipher is a type of cypher that combines multiple cryptographic techniques (like substitution and transposition) to encrypt data. offering a stronger security level than single transformation ciphers.

(g) what is the basic difference between feistel cipher and non-feistel cipher?

→ 1. Feistal cipher divide the plaintext into halves, while non-feistal ciphers do not.

2. Feistal ciphers apply the round function to one half, using the other half as input, while non-feistal ciphers apply the substitution-permutation network to the entire plaintext.

(h) what is proxy firewall?

5x2

2021

(a) what is meant by IP spoofing? what is phishing?

⇒ IP-spoofing

- Definition: IP spoofing is a cyber attack technique where an attacker ~~with~~ falsifies the source IP address in the header of an IP packet to disguish their identity or impersonate a trusted entity.

This deceives the recipient system into believing the packet originates from a legitimate sources.

Mechanism: In a network, every packet includes a source and destination IP address. Attackers use tools like Scapy (which is a packet crafting tool) to alter the

source IP field. since IP itself doesn't verify authenticity, the spoofed packet can bypass basic filters - unless additional security (e.g., Ingress filtering) is in place.

Example: In D-Dos attack, an attacker spoofs the victim's IP and sends requests to numerous servers. The servers reply to the victim, overwhelming it with traffic (e.g., the 2016 Dyn DNS attack used spoofing in parts of it's strategy).

Phishing

Definition: Phishing is a social engineering attack where attackers trick individuals into revealing sensitive information (e.g., passwords, credit card informations) by masquerading as a trustworthy entity, typically via fraudulent communication like emails or websites.

Mechanism: Attackers craft messages mimicking legitimate sources (e.g., a bank or tech company) with urgent or enticing prompts (e.g., "your account is compromised, click here to reset"). These lead to fake sites that capture user inputs or install malware.

Example: A spear phishing attack targets a CEO with a tailored email from "IT support" requesting login details for a "system update," leading to corporate data theft.

(b) Write briefly the categories of attacks.

⇒ In Information security, attacks are classified based on their intent, execution, and impact. Here are the main categories with detailed explanations:

- **Passive Attacks**: These focus on gathering information without altering system resources. Examples include eavesdropping (intercepting communications like wiretapping a network) and traffic analysis (inferring patterns from data flow, such as detecting high activity during a military operation). They're stealthy and hard to detect since no damage is done directly, threatening confidentiality.
- **Active Attacks**: These involve modifying data or disrupting systems. Subtypes include:
  - **Masquerade**: pretending to be a legitimate user (e.g., using stolen credentials to access a bank account).
  - **Replay**: Reusing captured data (e.g., resending a payment request to trick a server).
  - **Modification**: Altering data in transit (e.g., changing a bank transfer amount).
  - **Denial of service (DoS)**: overloading a system to deny access (e.g., flooding a website with requests).

- **Insider Attacks:** Launched by a authorised individuals, such as employees leaking sensitive data (e.g., an IT admin stealing customer records). These are dangerous due to internal access and trust, impacting confidentiality.

- **Outsider Attacks:** originate externally, like hackers exploiting vulnerabilities (e.g., using malware like ransomware to lock systems). These often target all security goals.

- **Example**

A hacker might use a passive ~~passwords~~ attack (sniffing wi-fi) to steal a password, then an active attack (masquerade) to log in and launch a DoS, showing how categories combine in real threats.

(c) ~~Explain the feistal cipher.~~

⇒ The feistal cipher is a symmetric encryption structure used in block cipher like DES (Data Encryption standard). It divides the plaint ext block into two halves (left and right). In each round:

(a) the right half is combined with a sub key (via a function f) and XORed with the left half.

b) The halves are swapped for the next round.

This process repeats for multiple rounds (e.g., 16 in DES). The design ensures reversibility: Decryption uses the same algorithm with subkeys in reverse order. Its strength lies in the confusion (via F) and diffusion (via swapping) it introduces.

(d) Explain the components of network security model. (~~65 - mark answer~~)

⇒ The network security model identifies key elements involved in securing communication. Its components are:

1. Sender: The entity sending data (e.g. a user or server). It initiates the process and applies security like encryption. For example, a customer sending payment details online.

2. Receiver: The intended recipient (e.g., a server or user). It verifies and processes the data, ensuring authenticity and integrity, like a bank receiving the payments.

3. Transmission medium: The channel data travels through (e.g., internet, wifi). It's vulnerable to interception, requiring protection like TLS to stay secure.

4. Security Mechanism: Tools and techniques (e.g., encryption, firewalls, hashing) that protect data's confidentiality, integrity, and availability, for instance, a firewall blocks unauthorized access.

5. Adversary: The threat secure (e.g., hackers) aiming to breach security via attacks like phishing or spoofing. Defenses are designed to counter this risk.

2022

(a) Explain the goals of using Information security. What is MAC?

⇒ Goals of IS

(a) Confidentiality: It ensures data is accessible only to the authorized parties (e.g., via encryption).

(b) Integrity: prevents unauthorized alteration of data (e.g., via hashing).

(c) Availability: Ensures systems/data are accable to authorized users when needed (e.g., mitigation DoS attacks).

(4) Authenticity: varifies the identity of users/ systems (e.g., via digital signatures)

⇒ Non-repudiation: prevents denial of actions (e.g., via signed ~~signatures~~ receipts).

MAC (Message Authentication Code)

A MAC is a cryptographic checksum, generated using a secret key and appended to a message. It ensures data integrity and authenticity by allowing the receiver to ~~verify~~ that the message hasn't been tempered with and comes from a legitimate source.

(b) The encryption key in a transposition cipher is (3, 2, 6, 1, 5, 4). Find the decryption key, with these key show the encryption and decryption process for the message "Information secrecy" [excluding blank space]. (5)

⇒ Message Preparation

"Information secrecy" remove blank space "Informationsecrecy" which is 18 characters.

Determine matrix size

since the length of the key is 6 and

the message length is 18, by dividing it with 6 we get 3, it means 6 columns and 3 rows.

- Craft the matrix

	1	2	3	4	5	6
1	I	n	f	o	r	m
2	a	t	i	o	n	s
3	e	e	r	@	e	y

~~Generate de~~

Encrypt it ~~with the~~.

Encrypt the message with the key [3,2,6,1,5,4]

f	n	m	i	r	o
i	t	s	a	n	o
r	e	y	e	e	@

So our Encrypted text is = "finmtesy iaernoo@"

- Find the Decryption key

E-key ⇒

3	2	6	1	5	4
1	2	3	4	5	6

⇒

1	2	3	4	5	6
4	2	1	6	5	3

So the decryption key is ⇒ 421653

Craft Matrix for Decryption

our cipher text ⇒ "firntemsy iaerncoore"

	1	2	3	4	5	6
1	f	r	m	i	r	o
2	i	t	s	a	n	o
3	r	c	y	e	c	e

Decrypt the matrix

D-key ⇒ [4, 2, 1, 6, 5, 3]

	4	2	1	6	5	3
1	i	r	f	o	r	m
2	a	t	i	o	n	s
3	e	c	r	e	c	y

Read row wise

"information seecrecy"

as we can see our Dekey gives us the real text/message.

Final Answer

⇒ message ⇒ "information seecrecy".

e-key → 3 2 6 1 5 4

emsg ⇒ "firntemsy iaerncoore".

d-key → 4 2 1 6 5 3

(c) Write two difference between symmetric key and asymmetric key encryption algorithm. With ~~key~~ suitable diagram explain the key generation process of DES algorithm.: (no table is required).

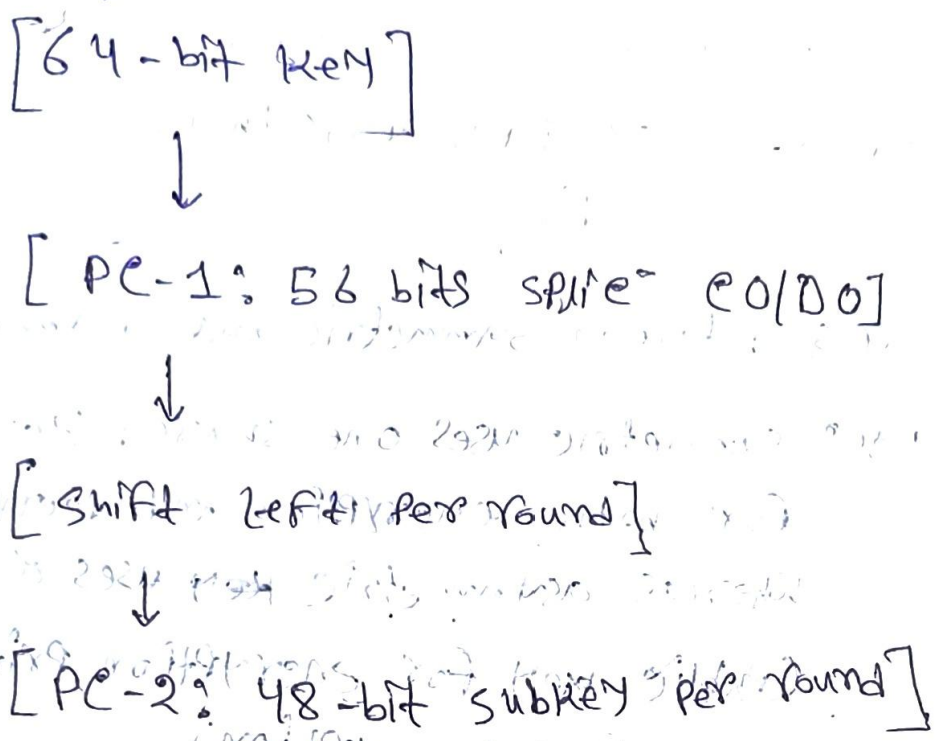
⇒ Differences between symmetric and asymmetric

- Key usage: Symmetric uses one shared key for both encryption and decryption: whereas asymmetric ~~key~~ uses a pair (public key for encryption, private key for decryption)
- Speed: Symmetric is faster (e.g., DES, AES); Asymmetric is slower due to complex math (e.g., RSA).

DES key generation algorithm

- Start with a 64-bit key including 8-parity bits.
- Step-1: Permuted choice 1 (PC-1): Discard parity bits, permute 56 bits into two 28-bit halves (C0, D0).
- Step-2: Left shifts: for each of 16 rounds. ~~for c~~ shift C0 and D0 left (1 or 2 bits, depending on rounds).
- Step-3: Permuted choice (PC-2): From shifted 56 bits, select 48 bits as the sub key for each round.

Diagram for DES key generation algorithm,



(d) Write properties of good hash functions. What is avalanche effect? Differentiate between attack and threat.

→ Properties of Good hash functions:

1) Pre-image Resistance: Hard to find input m given hash h(m).

2) Second pre-image Resistance: Hard to find $m' \neq m$ where $h(m') = h(m)$.

3) Collision Resistance: Hard to find $m1 \neq m2$ where $h(m1) = h(m2)$.

4) Deterministic: Same input will always produces same output.

5) Fast computation: Efficient to compute h(m).

• Avalanche Effect: it says that A small change in input (e.g.: 1 bit) causes a significant unpredictable change in hash output (ideally, ~50% bits flip), enhancing security.

Difference between Attack and threat

→ Threat: is a potential event or condition that could harm a system's security, representing a risk that may or may not occur.

Attack: An Actual Intentional act exploiting a vulnerability to cause harm, carried out by an adversary.

Nature

Threat: Passive and hypothetical. It's a possibility, like a weak password that could be exploited.

Attack: Active and executed. It's the realization of a threat, like a hacker using that weak password to gain access.

Example

Threat: unencrypted wi-fi in a cafe poses a risk of data interception.

Attack: A hacker performs a man-in-the-middle attack on that wifi to steal login credentials.

2022-23

@ Explain the concept of confusion and Diffusion.

⇒ Confusion and diffusion are fundamental principles in cryptography, introduced by Claude Shannon to ensure the security of ciphers.

Confusion: This refers to making the relationship between the plaintext and the ciphertext as complex and obscure as possible. The goal is to ensure that each bit of the ciphertext depends on several parts of the key in a convoluted way. This is typically achieved through substitution operations (e.g., S-boxes in modern ciphers like AES, DES). For example, if a single bit of the key changes, it should drastically alter the ciphertext making it hard for an attacker to deduce the key from the ciphertext.

Diffusion: This principle aims to spread the influence of a single plaintext bit over many bits of the ciphertext. The idea is to hide the statistical structure of the plaintext, making it difficult to identify patterns. Diffusion is often implemented through permutation or transposition operations (e.g., P-boxes). For instance changing one-bit in the plaintext should ideally affect multiple bits in the ciphertext, ensuring that small changes propagate widely.

(b) Explain the working principle of Feistel cipher (2021, e)

(c) Explain in brief the concepts of replay attack and repudiation. Which security goal is threatened by these two attacks?

⇒ Replay Attack: In a replay attack, an attacker intercepts a valid message (e.g., authentication data or transaction request) and retransmits it later to deceive the recipient. For example, if a user sends a bank transaction request, an attacker could replay it to repeat the transaction without authorization. This attack exploits the lack of freshness in communication. Countermeasures include time stamps, nonces, or session tokens to ensure messages are unique and time-bound.

Repudiation: Repudiation occurs when a party involved in a transaction or communication denies having participated in it. For instance, a sender might claim they never sent a message, or receiver might deny receiving it. This is common in digital transactions where proof of action is weak. Digital signatures and logging mechanisms are used to prevent repudiation by providing non-repudiable evidence.

Threatened Security Goal:

- Replay attacks threaten authentication and integrity, as they allow unauthorized reuse of valid data, undermining trust in the system.
- Repudiation threatens non-repudiation, a security goal ensuring that actions or messages can be undeniably linked to their originator/recipient.

Both attacks compromise the reliability and trustworthiness of secure communication systems.

(d) What is meant by IP-spoofing? What is phishing? (2021, a)*

10x1

(a) What are the requirements of cryptographic hash function?

- Pre-Image Resistance: Given a hash value (h), it should be computationally infeasible to find an input (m) such that (h = H(m)).

Second pre-Image Resistance: Given an input (m1), it should be computationally infeasible to find another input (m2) != (m1) such that H(m1) = H(m2).

Collison Resistance: It should be computationally infeasible to find any two distinct inputs m1 and m2 such that H(m1) = H(m2).

Efficiency: The hash function should be fast to compute for any input.

Fixed output length: The hash function produces a fixed-length output regardless of input size.

Deterministic: The same input always produces the same hash output.

Distinguish between diffusion and confusion.

→ Diffusion

Ensures that a small change in the input (e.g., flipping a single bit) result in a significant change in the output (e.g., changing roughly half the output bits). It spread the influence of input bits across the output. Example: Avalanche effects in hash functions.

Confusion

Make the relationship between the input and output complex and non-linear, obscuring the connection between plaintext and ciphertext. It relies on substitutions operations (e.g., S-boxes in AES).

Key Difference: Diffusion focuses on spreading changes (statistical), while confusion focuses on complicating the input-output relationship (structural).

(b) Describe HMAC Algorithm.

⇒ HMAC (Keyed Hash Message Authentication Code) combines a cryptographic hash function (e.g., SHA-256) with a secret key to provide both data integrity and authentication. The algorithm is as follows:

1) Input: Message (m), secret key (K), hash function (H).

2) Pad the key (K) to the block size of (H). If (K) is longer, hash it first: (K' = H(K)).

3) Define two constants:
- (ipad = 0x36) repeated to block size.
- (opad = 0x5C) repeated to block size.

4) Compute inner hash: (H((K' ⊕ ipad) || m)), where || denote concatenation.

5) Compute outer hash: (H((K' ⊕ opad) || H((K' ⊕ ipad) || m))).

6) Output: The final hash is the HMAC.

(b) Comment on security of HMAC.

→ Robustness: HMAC is secure as long as the underlying hash function is collison-resistant and has good randomness properties.

Key Protection: The use of (ipad) and (opad) ensures that even if the hash function has weaknesses, the key remains protected.

Resistance: Secure against length-extension attacks, unlike plain hash-based MACs.

2022

(a) Explain the Random oracle model briefly.

→ The Random oracle model is theoretical framework where a hash function is modeled as an idealized black box that produces as truly random output for each unique input. It assumes:

- Outputs are uniformly random and independent for distinct inputs.
- The function is efficiently computable but impossible to reverse-engineer without querying.

It's used to analyze cryptographic schemes (e.g., digital signatures) but is unrealistic in practice due to real hash function limitations.

(a) What is pre image, 2nd pre image and Collison attack?

→ Pre-image Attack: Given a hash value (h), find an output (m) such that (H(m) = h). Complexity: $O(2^n)$ for an n bit hash.

Second Pre-Image Attack: Given an input (m-1), find another input (m-2 != m-1) such that (H(m-1) = H(m-2)) Complexity: $O(2^n)$.

3 Collison Attack: Find any two distinct inputs (m_1 != m_2) such that H(m_1) = H(m_2) complexity: $O(2^{\frac{n}{2}})$ due to the birthday paradox

(b) Explain the features of firewall.

→ Traffic control: Filters incoming and outgoing network traffic based on predefined rules.

Access Control: Restricts unauthorized access to networks or systems.

Monitoring/Logging: Tracks network activity for auditing and detecting suspicious behavior.

(b) What is packet filtering firewall?

→ A packet filtering firewall examines packet headers (e.g., IP address, ports, protocols) and allows or denies packets based on rules. It operates at the network layer (layer 3)

(b) Briefly explain possible attacks and countermeasures on a packet filtering firewall.

→ 1) IP spoofing: Attackers forge source IP addresses to bypass rules.
- countermeasure: use ingress/egress filtering to validate IP addresses

2) Fragmentation Attacks: Malicious packets are split to evade detection.
- Countermeasure: Reassemble fragments before inspection or block fragmented packets.

3) Port Scanning: Attackers probe open ports to find vulnerabilities
- Countermeasure: Limit allowed ports and log scanning attempts.

4) SYN Flood: overwhelms the target with incomplete TCP connections.
- Countermeasure: use SYN cookies or rate-limiting.

5) Rule misconfiguration: weak rules allowed unintended traffic.
- Countermeasures: Regularly audit and test firewall rules.

6. Application-Layer Attacks: Exploit weakness not visibl at the packet level (e.g., SQL injection).
   - Counter measures: Combine with application-layer firewalls or IDS/IPS.

2022-23

(a) Describe HMAC Algorithm. (2021 b)

(a) How does HMAC is different from other cryptographic Hash functions?

1) Keyed vs unkeyed: HMAC requires a secret key, unlike hash functions like SHA-256, which are unkeyed and only ensure integrity.

2) Authentication: HMAC provides authenticity (verifying the sender), while Standard hash function do not.

3) Resistance to Attacks: HMAC is resistant to length-extension attacks, unlike plain hash functions (e.g., MD5, SHA-1).

(b) What is firewall? Briefly explain possible attacks and counter measures on a packet filtering firewall: (2022-b)

2023-24 / 1x5

(1)

(a) Write two critical characteristics of information.

→ Confidentiality:- Ensures that information is accessible only to those authorised to have access.

Integrity :- Ensures the accuracy and completeness of the data and that it has not been tampered with.

(b) what do you mean by decryption?

→ Decryption is the process of converting encrypted (cyphertext) data back into it's original (plaintext) form using a key or algorithm.

(c) what is firewall?

→ A firewall is a security system (hardware or software) that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

(d) write difference between virus and worm.

→ Virus: Attaches itself to a program or file and spreads when the file is executed.

Worm: self-replicates and spreads through networks without needing to attach to a file.

(e) what is spoofing?

→ Spoofing is a cyber attack where an attacker impersonates another device or user to gain access to sessitive data or systems.

(f) Define digital signature.

⇒ A digital signature is a cryptographic technique used to validate the authenticity and integrity of a message, software, or digital document.

(g) What is phishing attack?

⇒ Phishing is a type of cyber attack where attackers trick individuals into revealing sensitive information (like passwords or credit card details) by pretending to be a trust worthy entity via email, messages, or websites.

(h) What is residual risk?

⇒ Residual risk is the amount of risk that remains after security measures have been applied to reduce or eliminate threats.

Ex 2

(a) Explain goals of using Information security.

⇒ Goals of Information security is the CIA Triad.

where C → Confidentiality
I → Integrity
A → Availability

Let's discuss about each,

Confidentiality

- Ensures that sensitive data is accessed only by authorized individuals.
- Methods include encryption encryption, access control, and authentication.
- Example: Password-protected files or encrypted emails.

Integrity

- Maintains Accuracy and consistency of data during storage, transmission, and processing.
- Prevents unauthorized modification of data.
- Example: use of checksums or digital signatures.

Availability

- Ensures that systems and data are accessible when needed by authorized users.
- Protection against attacks like DDoS, and system failures is necessary.
- Example: using redundant systems and network backups.

Additional goals

Authentication: verifies the identity of users or systems before granting access

Non-repudiation: Ensures that a sender can't deny sending a message, often through digital signatures.

(a) what is MAC?

→ Message Authentication code (MAC); is a cryptographic code generated using a secret key and message. It ensures:

- Message Integrity (no tampering),
- Authentication (message is from a legitimate source).

formula:

$$MAC = H(K, M)$$

where, H = hash function,
K = secret key
M = Message.

(b) The decryption key in transposition cipher is (6, 2, 1, 5, 3, 4). Find the encryption key. ~~Explain~~

→ Given decryption key: [6, 2, 1, 5, 3, 4]

This means,

- 1st position of ciphertext comes from 6th position of plaintext.
- 2nd from 2nd, 3rd from 1st, and so on.

lets reverse the mapping:

1,	2,	3,	4,	5,	6	→	1,	2,	3,	4,	5, 6
6,	2,	1,	5,	3,	4		3,	2,	5,	6,	4, 1

So the encryption key is ⇒ [3, 2, 5, 6, 4, 1]

(b) Explain the rail fence cipher with suitable example.

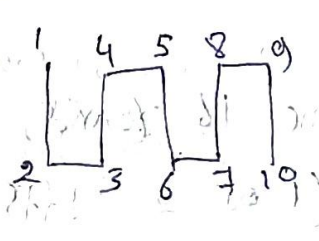
→ ~~A form of~~ Rail fence cipher is A form of transposition cipher where characters of the plaintext are written diagonally in a zig-zag pattern, across multiple rails (lines), then read row by row.

Example

plaintext → Hello World

1. write in rails

H		L		O		O		L	
	E		L		W		R		D



2) now read row wise → HLOOL ELWRD

(c) write two difference between symmetric key and asymmetric key encryption.

Symmetric	Asymmetric
used same key for encryption and decryption.	uses a pair of keys - public and private
Faster and suitable for bulk data	slower, used for secure communication
Example: AES, DES	Example: RSA, ECC
Requires key sharing	No need to share private key.

(c) write suitable diagram explain key generation of DES.

⇒ DES (Data Encryption Standard) uses a 56-bit key (from original 64-bit, 8 bits are parity).

Steps:

1) Initial permutation (PC-1)
   - 64-bit key is permuted into 56 bits.

2) splitting:
   - 56-bit key is split into two halves (28 bits each): C0 and D0

3) Shifting:
   - For each of the 16 rounds, the halves are shifted left (1 or 2 bits depending on round).

4) Compression permutation (PC-2):
   - Each round key is compressed from 56 to 48 bits.

5) output:
   - 16 sub keys (48 bits each) are generated one for each round of DES.

(d) Distinguish between Dos and D-Dos attack.

→ Dos vs DDos

→ single source sends traffic | Multiple sources send traffic

Easier to trace and block | Harder to trace due to many sources.

Example: ping of death | Example: Botnet-based flooding attack.

(d) for a multiplicative cipher, encryption key is 11. Find the decryption key.

→ Encryption key = 11

Modules = 26 [Standard English alphabet]

we need to find decryption key d such that:

$(11 \times d) \bmod 26 = 1$

trying values:

$11 \times 19 = 209$

$209 \% 26 = 1$

decryption key = 19

(e) What do you mean by crypto analysis?

→ cryptography is the science of analysing and breaking cryptographic systems

- It involves finding weaknesses or patterns in encryption schemes
- Types of attacks include: brute force, frequency analysis, chosen plaintext, etc
- cryptographic analysis aim to retrieve the plaintext or key without authorized access.

10x1 (3)

Q Describe HMAC Algorithm?

→ HMAC (Hash-based message Authentication code) is a type of message Authentication code (MAC) that uses a cryptographic hash function and a secret key.

Purpose:

To ensure integrity and authenticity of a message during transmission.

Formula

$$HMAC(K, m) = H((K' \oplus opad) \,||\, H((K' \oplus ipad) \,||\, m))$$

where:

H = hash function (e.g., SHA-256, MD5)

K' = secret key (if shorter than block size, padded if longer, hashed)

m = original message

⊕ = XOR operation

opad = outer padding (0x5c repeated)

ipad = inner padding (0x36 repeated)

|| = concatenation

Steps of HMAC Algorithm:

a) If the K is longer than the block size of the hash function (e.g., 64 bytes for SHA-256, SHA3)

a. Resistant to length extension attacks, unlike plain hash(M || K)

- If a secret key remains secure, HMAC is computationally infeasible to break.
- Widely used in secure protocols:
  - HTTPS
  - SSL/TLS
  - IPsec
  - JWT (Json Web Tokens)

Advantages

- Efficient
- Secure
- Easy to Implement
- works with any cryptographic hash function.

(b) Distinguish between modern and traditional symmetric key cipher. Define a P-Box. Explain the three variations with suitable example. Which variation is invertible?

Traditional vs modern symmetric key cipher

Feature	Traditional cipher	modern cipher
Techniques used	Substitution & Transposition	complex mathematical operations
Block vs stream	Its stream based means perse character wise	It works on blocks (Block ciphers)
Security level	weak (easy to break	strong (resistant to bruteforce)
Key size	small 1 or 2 characters	large (128, 192, 256 bits)

Example	Caesar cipher, Playfair, Rail Fence	DES, AES, Blowfish

P-Box

A P-Box is used in block ciphers to perform permutation (re-ordering) of bits.

- It spreads the influence of each input bit across multiple output bits
- Helps in achieving diffusion, one of the principles of a secure cipher.

Three variations of P-Box

1) Straight P-Box
   - Rearranges bits without changing their values
   - Example:
     Input = [1,2,3,4,5,6,7,8]
     P-Box = [3,1,4,7,2,5,8,6]
     output = 3rd, 1st, 4th ... bit in order
2) Compression P-Box
   - Maps a large number of bits to a smaller number.
   - used in key generation or reducing redundancy
   - Example: 64-bit input → 48-bit output (as in DES key scheduling)
3) Expension P-Box
   - maps a fewer bits to more bits (some bits are duplicated
   - Helps in increasing the confusion before applying substitution.
   - Example: 32-bit input → 48-bit output (in DES)

Which variation is Invertible

- Straight P-Box is Invertible
- Because it is just rearrangement of bits, the original can be recovered by reversing the permutation.
- Compression and Expension P-Boxes are not invertible due to information loss or duplication.

Example

Suppose P-Box = (4,2,1,3)

Input bits = 1101 (positions 1,2,3,4)

After P-Box:

- Bit 4 → Position 1 → 1
- Bit 2 → Position 2 → 1
- Bit 1 → Position 3 → 1
- Bit 3 → Position 4 → 0

Output = 1110

Reverse P-Box will recover original input (invertible).