Q.l (a) State the definitions of Cryptography, Security and Steganography. Classify security attacks with brief explanation.

Ans: a)

1. Cryptography: Cryptography is the practice of secure communication in the presence of third parties or adversaries. It involves the use of mathematical algorithms to transform plaintext into ciphertext, making the information unreadable to anyone except the intended recipient who possesses the key to decrypt the message.
2. Security: Security is the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It is an essential requirement for ensuring privacy, confidentiality, integrity, and availability of data, networks, and computing systems.
3. Steganography: Steganography is the practice of concealing a secret message within another message or file without revealing its presence. It involves embedding the hidden message within the carrier file in such a way that it is not detectable by the naked eye or any detection tool.

Classifications of security attacks:

1. Passive attacks: Passive attacks are those attacks where the attacker monitors or eavesdrops on the communication between the two parties, but does not modify or disrupt the communication.
2. Active attacks: Active attacks are those attacks where the attacker modifies or disrupts the communication between the two parties.
3. Insider attacks: Insider attacks are those attacks where the attacker has authorized access to the system or network and abuses this access to compromise the security of the system.
4. Outsider attacks: Outsider attacks are those attacks where the attacker does not have authorized access to the system or network and tries to gain access by exploiting vulnerabilities in the system or network.
5. Distributed attacks: Distributed attacks are those attacks where multiple attackers collaborate to launch a coordinated attack on the system or network.

(b)Explain five ingredients of symmetric encryption scheme with appropriate figure.

Ans: b)

The five ingredients of a symmetric encryption scheme are:

1. Plaintext: This is the original message that is to be encrypted.
2. Encryption algorithm: The encryption algorithm is a mathematical function that transforms the plaintext into ciphertext using a secret key.
3. Secret key: The secret key is a sequence of bits that is known only to the sender and the receiver of the message. It is used by the encryption algorithm to transform the plaintext into ciphertext and vice versa.
4. Ciphertext: This is the encrypted message that is produced by the encryption algorithm using the plaintext and the secret key.
5. Decryption algorithm: The decryption algorithm is a mathematical function that transforms the ciphertext back into plaintext using the secret key.

Here is an example figure of a symmetric encryption scheme: 

In this figure, the plaintext is encrypted using an encryption algorithm and a secret key to produce the ciphertext. The ciphertext is then transmitted to the receiver, who uses the secret key and a decryption algorithm to transform the ciphertext back into plaintext.

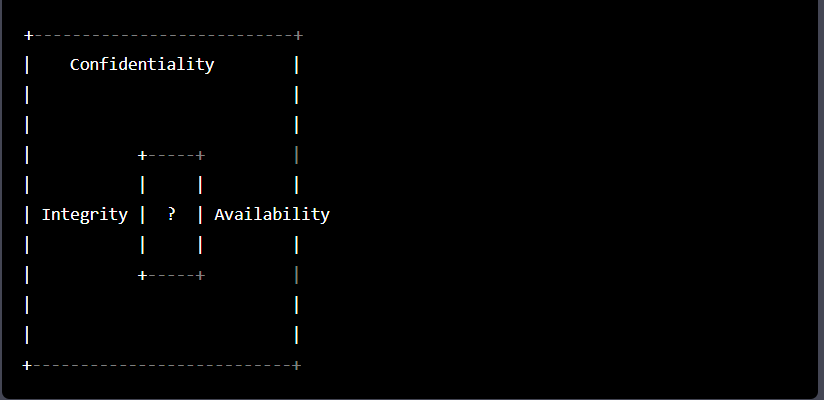
 Describe the procedures of transposition cipher. Draw the CIA triad.

(a) Procedures of transposition cipher: A transposition cipher is a cryptographic technique that rearranges the characters in a message to create a ciphertext. The following are the procedures for transposition cipher:

1. Choose a keyword or key phrase: A keyword or key phrase is chosen to determine the order of the columns and rows.
2. Write the message in a grid: The message is written out in a grid, with the number of columns determined by the length of the keyword.
3. Rearrange the columns: The columns of the grid are rearranged according to the order of the letters in the keyword.
4. Read the message row by row: The message is read out row by row, resulting in the ciphertext.

CIA triad: The CIA triad is a model that is used to describe the security objectives of confidentiality, integrity, and availability. These objectives are essential for any security system, and they help ensure that data is secure and protected. The CIA triad stands for:

* Confidentiality: ensuring that data is only accessible to authorized users and is protected from unauthorized disclosure.
* Integrity: ensuring that data is accurate, complete, and reliable, and that it is not tampered with or modified in any way.
* Availability: ensuring that data is accessible to authorized users when they need it and that it is not lost or destroyed.

 5

(b) i) Construct a Playfair Illatrix with the key happiness. 5 ii) Using this Playfair matrix of (i) encrypt and decrypt the following message:

Have a nice time.

(b) i) Playfair Illatrix with the key happiness:

H A P Y E

S I L O N B

C D F G K

M Q R T U

V W X Z

ii) Using this Playfair matrix of (i) encrypt and decrypt the following message: Have a nice time.

To encrypt "Have a nice time", we break it down into pairs of letters, like this:

HA VE AN IC ET IM E

We then use the Playfair matrix to find the corresponding ciphertext letters for each pair:

HA -> AP

VE -> WB

AN -> ND

IC -> CK

ET -> XZ

IM -> RX

E -> Y

The ciphertext for "Have a nice time" is "APWBNDCKXZRY".

To decrypt the ciphertext, we simply reverse the process:

AP -> HA

WB -> VE

ND -> AN

CK -> IC

XZ -> ET

RX -> IM

Y -> E

The plaintext for "APWBNDCKXZRY" is "HAVEANICETIME".

 Differentiate between block and stream ciphers.

(a) The main difference between block and stream ciphers is in how they encrypt data:

* Block ciphers: A block cipher encrypts a fixed-length block of data at a time. The block size is usually 64 or 128 bits. The plaintext is divided into blocks, each block is encrypted separately using the same key, and the resulting ciphertext blocks are combined. Examples of block ciphers include AES, DES, and Blowfish.
* Stream ciphers: A stream cipher encrypts data one bit or byte at a time. A stream cipher generates a stream of pseudorandom bits or bytes that are combined with the plaintext using XOR operation. The same key is used to generate the pseudorandom stream and to decrypt the ciphertext. Examples of stream ciphers include RC4, ChaCha20, and Salsa20.

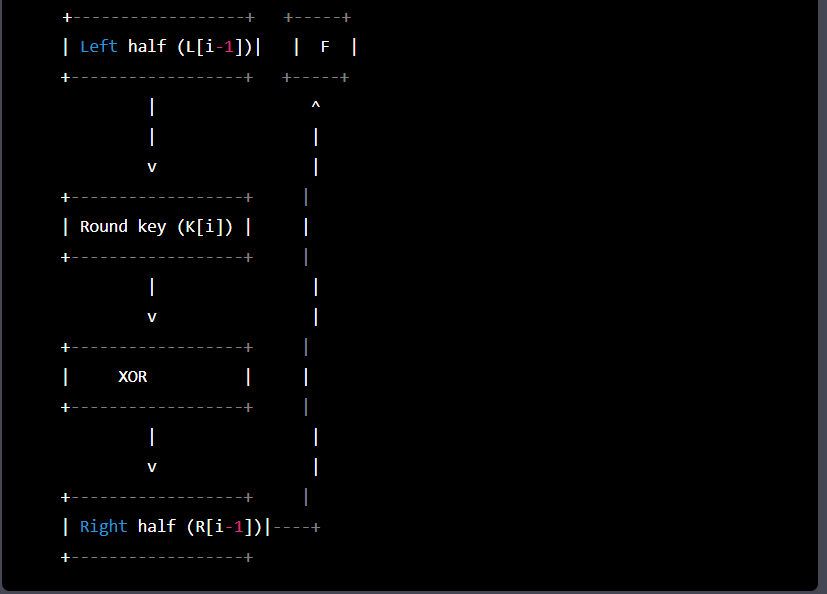
2

* 1. Draw the Feistel cipher structure. 3

(b) The Feistel cipher structure is a widely used design for block ciphers. It was invented by Horst Feistel in the 1970s and has been used in many cryptographic algorithms, including DES and Blowfish. The Feistel cipher structure consists of the following steps:

* The plaintext is divided into two halves.
* The left half is XORed with a round key.
* The result is fed into a round function that takes the right half as input and produces a new right half as output.
* The new right half is XORed with the left half from step 1.
* The left and right halves are swapped, and the process is repeated for a fixed number of rounds.
* Finally, the two halves are combined to produce the ciphertext.

Here is a diagram of the Feistel cipher structure:



* 1. Derive two keys for S-DES scheme for the following values: 5

i) 10-bit key as input key: 10101 101 10

 Two permutation function 10 and 8 as follows

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | |  | |  | | p 10 | | | | | | | | |
| I | | 5 | | 8 | | 9 | |  | 10 |  |  | |  | |  | |
|  | |  | |  | |  | |  | | |  | | | |
| 6 | | 5 | | 7 | | 4 | | 8 | 3 | | 10 | |  | |

(c) To derive two keys for the S-DES scheme using a 10-bit input key and the given permutation functions, we follow these steps:

1. Apply the P10 permutation to the input key:

Input key: 10101 1011 0 P10: 3 5 2 7 4 10 1 9 8 6 P10 key: 1 0 1 0 1 0 1 0 1 1

1. Split the P10 key into two halves of 5 bits each:

Left half: 1 0 1 0 1 Right half: 0 1 0 1 1

1. Apply the LS-1 (left shift by one) operation to each half:

Left half: 0 1 0 1 1 Right half: 1 0 1 1 0

1. Combine the two halves into a 10-bit key:

LS-1 key: 0 1 0 1 1 1 1 0 1 1

1. Apply the P8 permutation to the LS-1 key to derive the first subkey:

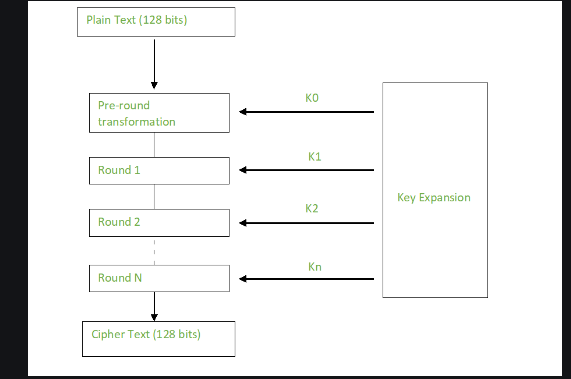
LS-1 key: 0 1 0 1 1 1 1

Q) Sketch the overall structure of AES.

(a) The overall structure of AES (Advanced Encryption Standard) consists of several components:

* Key expansion: The 128-bit key is expanded into a set of round keys.
* Initial round: The input plaintext is XORed with the first round key.
* Rounds: A fixed number of rounds are performed, each consisting of several transformations: SubBytes, ShiftRows, MixColumns, and AddRoundKey.
* Final round: The final round is similar to a round, but without the MixColumns transformation.
* Output: The final output is the ciphertext.

Here is a diagram of the AES structure:



4 (b) Apply the shift row transformations for the following state: 3

|  |  |  |  |
| --- | --- | --- | --- |
| 63 | C9 | FE | 30 |
| A2 | B5 | 67 | D4 |
| EF | 3C | 5E | 32 |
| AB | CD | EF | 21 |

* 1. Ans: To apply the ShiftRows transformation to the given state, we shift the second row one byte to the left, the third row two bytes to the left, and the fourth row three bytes to the left. Here is the resulting state:

Shifted Rows:



* 1. AES is more secured than DES. Justify it. Define Blowfish. 3

Ans: (c) AES is more secure than DES for several reasons:

* AES uses a larger key size than DES, which makes it more resistant to brute-force attacks.
* AES uses a more complex encryption algorithm than DES, which makes it harder to analyze and break.
* AES has a stronger security margin than DES, meaning that it is less vulnerable to attacks that exploit weaknesses in the cipher.
* AES has a longer lifespan than DES, as it is still considered secure and widely used, while DES is now considered outdated and insecure.

Blowfish is a symmetric-key block cipher designed by Bruce Schneier in 1993. It uses a variable-length key up to 448 bits and a 64-bit block size. Blowfish operates by dividing the input into blocks of 64 bits and encrypting each block separately. It uses a Feistel network with up to 16 rounds, each consisting of a substitution step, a permutation step, and a key mixing step. Blowfish is widely used in many applications, including encryption software, VPNs, and secure email services.

Q.5 (a) List the key component of internet mail structure. What is the difference between S/MIME and OpenPGP?

(a) The key components of internet mail structure are:

* Mail user agent (MUA): The software used by the user to create and read email messages.
* Mail submission agent (MSA): The software responsible for receiving email messages from MUAs and forwarding them to the mail transfer agent (MTA).
* Mail transfer agent (MTA): The software responsible for routing email messages between mail servers on the internet.
* Mail delivery agent (MDA): The software responsible for delivering email messages to the recipient's mailbox.
* Mail access agent (MAA): The software responsible for providing access to the recipient's mailbox.

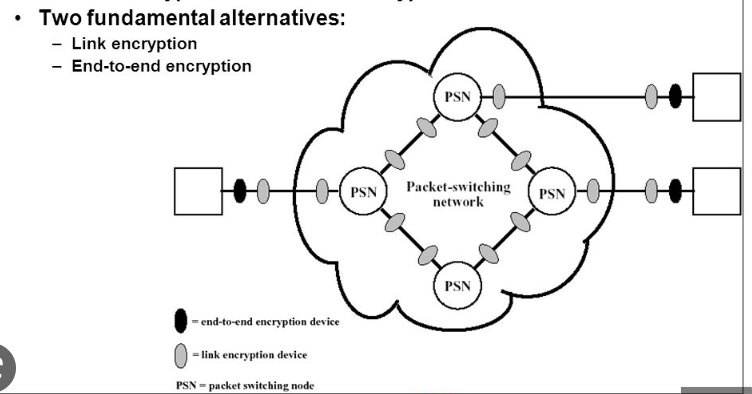
S/MIME (Secure/Multipurpose Internet Mail Extensions) and OpenPGP (Open Pretty Good Privacy) are both encryption standards used for securing email messages, but they differ in several ways. S/MIME is a standard developed by the Internet Engineering Task Force (IETF) and is supported by most email clients. It uses X.509 certificates for public key encryption and digital signatures. OpenPGP, on the other hand, is an open-source standard that uses a web of trust model for public key encryption and digital signatures. It is supported by a smaller number of email clients, but it is more flexible and can be used for other applications beyond email.

(b) What is traffic padding and what is its purpose? Show the differences exist between link and end-to-end encryption approaches using appropriate diagram.

(b) Traffic padding is the process of adding extra data to a message to make it a fixed length, in order to obfuscate the true message length and make it harder for an attacker to determine the size of the original message. The purpose of traffic padding is to increase the security of encrypted messages by preventing attacks such as traffic analysis and ciphertext-only attacks.

The main difference between link and end-to-end encryption approaches is the location where encryption and decryption occur. Link encryption occurs at the physical or data link layer of the network, while end-to-end encryption occurs at the application layer. In link encryption, data is encrypted as it is transmitted over the network, but it is decrypted before it reaches its final destination. This means that the data is still vulnerable to attacks while it is decrypted and in transit between network nodes. In contrast, end-to-end encryption encrypts data at the sender's device and decrypts it at the receiver's device, ensuring that the data is secure throughout its entire journey over the network.

Here is a diagram illustrating the differences between link and end-to-end encryption approaches:



(c)Show the taxonomy of malicious program.

 The taxonomy of malicious program includes:

1.Virus: A virus is a program that can replicate itself and infect other programs and files on a computer.

2.Worm: A worm is a self-replicating program that spreads across networks and can cause damage to computers and networks.

3.Trojan: A Trojan is a program that appears to be legitimate but contains malicious code that can harm a computer or steal sensitive data.

4.Ransomware: Ransomware is a type of malware that encrypts a user's files and demands payment in exchange for the decryption key.

5.Spyware: Spyware is a type of malware that can monitor a user's computer activity and steal sensitive data.

6.Adware: Adware is a type of malware that displays unwanted ads or pop-ups on a user's computer.

7.Rootkit: A rootkit is a type of malware that hides its presence and can give an attacker unauthorized access to a computer or network.

8.Botnet: A botnet is a network of compromised computers that can be controlled by an attacker to perform malicious activities, such as sending spam or launching DDoS attacks.

Q.6 (a)What are the types of intruders? State the definition of IPS and IDS.

(a) Types of Intruders:

Hackers: individuals or groups who break into computer systems with malicious intent, often to steal data or cause damage.

Insiders: employees or contractors who have access to sensitive information and abuse their privileges to gain unauthorized access.

Cybercriminals: individuals or groups who use the internet to commit crimes such as identity theft, fraud, and extortion.

Script kiddies: individuals with limited technical skills who use pre-made tools and scripts to launch attacks.

State-sponsored attackers: individuals or groups backed by government entities to carry out cyber espionage, sabotage or disruption.

IPS and IDS:

Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) are two types of security tools used to detect and prevent attacks in computer networks.

IDS is a security tool that monitors network traffic for signs of potential threats or unauthorized access attempts. It analyzes the traffic patterns, protocols and behavior of the network and alerts the security team if it detects any suspicious activity. IDS can be deployed in various ways such as network-based, host-based, or application-based.

IPS, on the other hand, not only detects suspicious activity but also takes proactive measures to prevent attacks. It can automatically block or quarantine suspicious traffic or perform other actions to prevent potential threats.

(b) Classify and explain IDS.

(b) Types of IDS:

Network-based IDS: Monitors network traffic and analyzes data packets to detect suspicious activity. It is placed at the perimeter of the network.

installed on the individual host machines and can detect attacks that may not be visible at the network level.

Application-based IDS: Monitors specific applications and their logs to detect and prevent unauthorized access attempts.

Anomaly-based IDS: Monitors network traffic for abnormal activity or deviations from normal behavior, as opposed to matching specific attack patterns.

Signature-based IDS: Compares network traffic with known attack signatures and alerts when it finds a match.

(c) What do you mean by password vulnerabilities?

Password vulnerabilities refer to weaknesses in passwords that make them easier to crack or guess, leaving the user's accounts and data vulnerable to unauthorized access. Common password vulnerabilities include using easily guessable passwords, using the same password for multiple accounts, and not changing passwords regularly. Attackers can use a variety of techniques to exploit password vulnerabilities, such as brute force attacks, dictionary attacks, and social engineering. To mitigate these risks, users are advised to create strong, unique passwords, use two-factor authentication, and change their passwords regularly.

Q.7 (a) Why public-key cryptography is necessary? What are the requirements for message authentications are followed when communications across a network?

(a)

 Public-key cryptography is necessary because it allows secure communication over an insecure channel without requiring both parties to share the same secret key. In a public-key system, each party has a public key and a private key. The public key can be shared with anyone, while the private key must be kept secret. When a sender wants to send a message to a receiver, they encrypt the message using the receiver's public key, which can only be decrypted with the receiver's private key. This ensures that only the receiver can read the message.

The requirements for message authentication when communicating across a network include:

Data integrity: ensuring that the message has not been modified or tampered with during transmission.

Authenticity: ensuring that the message is from the claimed sender and has not been forged or impersonated.

Non-repudiation: ensuring that the sender cannot deny having sent the message.

Confidentiality: ensuring that the message contents are kept secret from anyone who is not the intended recipient.

(b) Perform encryption and decryption using RSA algorithm with p=3, q=7, e=9 and n=5.

(b)Given: p=3, q=7, e=9, n=5

First, we need to calculate n and φ(n):

n = p \* q = 3 \* 7 = 21

φ(n) = (p-1) \* (q-1) = 2 \* 6 = 12

Next, we need to find d, the private key:

d \* e ≡ 1 (mod φ(n))

d \* 9 ≡ 1 (mod 12)

One solution for d is 5:

5 \* 9 ≡ 45 ≡ 1 (mod 12)

Therefore, the public key is (e, n) = (9, 21) and the private key is d = 5.

To encrypt a message M = 13, we use the following formula:

C = M^e mod n

C = 13^9 mod 21 = 20

So the encrypted message is 20.

To decrypt the message, we use the following formula:

M = C^d mod n

M = 20^5 mod 21 = 13

So the decrypted message is 13.

Q.8 (a) Apply Hill cipher where key is (hill) and plain text is HAPPY, find the cipher text.

(a) Applying Hill cipher with key "hill" and plaintext "HAPPY":

First, we need to convert the letters to numbers using the following mapping:

A = 0, B = 1, C = 2, ..., Z = 25

HAPPY becomes 7 0 15 15 24

Next, we need to break the plaintext into blocks of size 2, since the key is a 2x2 matrix:

[H A] [P P] [Y \_]

The last block only has one character, so we add a padding character (in this case, an underscore).

Now we can multiply each block by the key matrix, and take the result modulo 26 to get the corresponding ciphertext block:

[H A] \* [7 8] = [25 0] [P P] [11 7] [1 3] [Y \_] [18 11]

The resulting ciphertext is:

ZBBDSE

Therefore, the ciphertext for the plaintext "HAPPY" using Hill cipher with key "hill" is "ZBBDSE".

(b) Explain the pros and cons of steganography techniques in the field of multimedia security.

(b) Pros and Cons of Steganography Techniques in Multimedia Security:

Pros:

·       Steganography can provide a high level of security by hiding sensitive information within other files, making it difficult for attackers to detect or intercept.

·       It is a relatively simple and cost-effective method of securing information compared to other encryption techniques.

·       Steganography can be used to protect a wide range of multimedia files, including images, audio, and video.

Cons:

·       Steganography techniques can be detected by skilled attackers, particularly if the embedded message alters the original file's characteristics.

·       Steganography can only protect against unauthorized access to the information, and it does not protect the information from being modified or deleted.

·       Embedding a hidden message in a multimedia file can reduce the file's quality or affect its performance, which can be a problem in some applications.

(c) What is block cipher? Explain the working principle of block cipher algorithms.

(c) Block Cipher : Block cipher is a cryptographic algorithm that encrypts a fixed-sized block of data (usually 64 or 128 bits) at a time. It divides the plaintext into blocks and uses a key to transform each block into a ciphertext block of the same size.

The working principle of block cipher algorithms involves several steps:

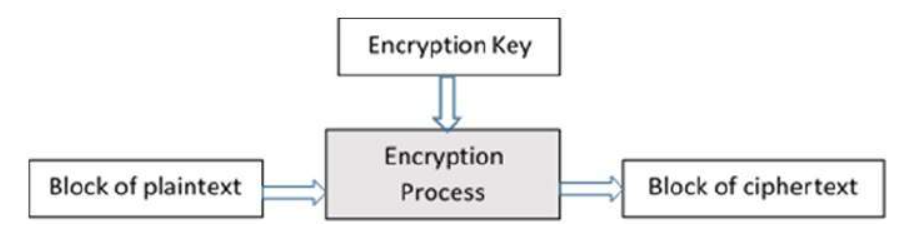
1. Substitution: In this step, the plaintext block is substituted with a different block of data using a substitution box (S-box) based on the key.

2. Permutation: The substitution output is then permuted or shuffled using a fixed pattern to create a new block.

3. Key Mixing: The permuted block is then mixed with the key using an exclusive OR (XOR) operation.

4. Iteration: The previous three steps (substitution, permutation, and key mixing) are repeated several times (typically 10-16 rounds) to create a highly secure and complex cipher.

Examples of block cipher algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES). Block cipher algorithms are widely used in secure communication, electronic payment systems, and other applications that require high levels of security.

****