What is cryptanalysis? Summarize the various types of cryptanalytic attacks on encrypted messages.

Step 1:

Cryptanalysis is the technique of examining cryptographic systems for flaws or information leakage.

Cryptanalysts, for example, aim to decipher cipher texts without having access to the plaintext source, encryption key, or encryption algorithm; they also attack safe hashing, digital signatures, and other cryptographic procedures.

Step 2:

Types of Attacks

* Known-Plaintext Analysis (KPA) : In this type of attack, some plaintext-ciphertext pairs are already known. ...
* Chosen-Plaintext Analysis (CPA) :
* Ciphertext-Only Analysis (COA) :
* Man-In-The-Middle (MITM) attack : ...
* Adaptive Chosen-Plaintext Analysis (ACPA) :

Step 3:

Known-Plaintext Analysis (KPA): Some plaintext-ciphertext pairs are already known in this sort of attack. In order to find the encryption key, the attacker maps them. This assault is simpler to execute because a large amount of data is already available.

CPA (Chosen-Plaintext Analysis): In this sort of attack, the attacker selects random plaintexts, obtains the accompanying cipher texts, and attempts to decrypt the data. It's similar to KPA in that it's easy to execute, but the success rate is low.

COA (Cipher Text-Only Analysis): In this form of attack, the attacker only knows a portion of the cipher text and attempts to deduce the encryption key and plaintext. It is the most difficult to implement, but it is also the most likely attack because just cipher text is required.

Man-In-The-Middle (MITM) attack:

The attacker intercepts the message/key between two communicating parties through a secured channel in a Man-In-The-Middle (MITM) attack.

ACPA (Adaptive Chosen-Plaintext Analysis)

It is a variant of CPA. After obtaining cipher texts for certain plaintexts, the attacker requests the cipher texts of further plaintexts.

**List the parameters of a symmetric block cipher for greater security.**

Step 1:

A symmetric cypher is one that encrypts and decrypts using the same key. Asymmetric or symmetric cyphers or algorithms exist. Symmetric ones employ the same key (sometimes referred to as a secret key or private key) to convert plaintext into ciphertext and vice versa.

Step 2:

The symmetric block cypher is determined by the parameters and design elements used.

• Block size: Larger block sizes provide more security but slow down encryption and decoding.

• Key size: A larger key size provides more security, but it may slow down encryption and decoding. In current algorithms, the most frequent key length is 128 bits.

• Number of rounds: A symmetric block cipher's essential is that a single round provides insufficient security, but numerous rounds provide increased security. 16 rounds is a common size.

• Subkey generation algorithm: A higher level of complexity in this process should make cryptanalysis more challenging.

• Round function: Once again, increased complexity equates to better cryptanalysis resistance.

• Fast software encryption/decryption: As a result, the algorithm's speed of execution and hardware implementation become a factor.

**What is a block cipher? Name the important symmetric block ciphers.**

Step 1:

A block cypher is an encryption method that encrypts a block of text using a deterministic algorithm and a symmetric key, rather than encrypting one bit at a time like stream cyphers. AES, for example, is a popular block cypher that encrypts 128-bit blocks with a key length of 128, 192, or 256 bits.

Step 2:

The symmetric block cyphers Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are both used to encrypt data. IBM created the DES block cypher in 1975, which consisted of 64-bit blocks and a 56-bit key.

Step 3:

DES is a symmetric key block cypher that uses a 64-bit block size and a 64-bit key size. It is vulnerable to some types of attacks, hence it isn't widely used.

The Advanced Encryption Standard (AES) is a symmetric block cypher that the United States government has chosen to safeguard confidential information. AES is used to encrypt sensitive data in software and hardware all over the world. It's critical for government computer security, cybersecurity, and data security.

**There are two applications for public-key cryptography:**

Step 1:

1) Encryption with the recipient's public key (the message is encrypted with the recipient's public key and can only be decoded with the recipient's private key)

The approach of encrypting data with two separate keys and making one of the keys, the public key, available for anybody to use is known as public key encryption or public key cryptography. The private key is the other of the two keys.

Step 2:

Every user's public key is stored in the Public Key Register. If B wants to transmit a confidential message to C, B uses C's public key to encrypt the message. When C receives the message from B, it can use its own Private key to decrypt it.

Because users never have to transmit or reveal their private keys to anyone, public key cryptography remains the most secure protocol (over private key cryptography). This reduces the odds of cyber criminals discovering an individual's secret key during transmission.

2)Digital signature

A mathematical algorithm is frequently used to confirm the validity and integrity of a message using a digital signature, which is a sort of electronic signature (e.g., an email, a credit card transaction, or a digital document).

Public key cryptography, often known as asymmetric cryptography, is used to create digital signatures. Two keys are produced using a public key algorithm like RSA (Rivest-Shamir-Adleman), resulting in a mathematically connected pair of keys, one private and one public.