Q10.

Both Cipher text only and Known Plaintext attacks are types of cryptographic attacks that aim to break the security of a cipher or encryption system. Here's an illustration of each:

**Cipher text only attack**

In a Cipher text only attack, the attacker only has access to the encrypted messages (the cipher text) but does not have any knowledge of the corresponding plain text. The goal of the attack is to analyze the cipher text and deduce some information about the original message or the encryption key.

For example, suppose an attacker intercepts a series of encrypted messages exchanged between two parties. The attacker can analyze the frequency of characters and patterns in the cipher text to deduce some information about the language used in the original message. The attacker can also perform statistical analysis to determine if certain words or phrases are likely to appear in the original message.

One common technique used in Cipher text only attacks is known as frequency analysis. This technique involves analyzing the frequency of characters or character pairs in the cipher text to identify patterns that may correspond to common letters or words in the original message. The attacker can then use this information to make educated guesses about the plaintext or encryption key.

**Known plaintext attack**

In a Known plaintext attack, the attacker has access to both the cipher text and some corresponding plain text. The goal of the attack is to analyze this information to deduce the encryption key or to be able to decrypt additional messages encrypted with the same key.

For example, suppose an attacker intercepts an encrypted message and also knows the corresponding plain text for that message. The attacker can use this information to deduce the encryption key by comparing the plain text to the cipher text. The attacker can then use this key to decrypt additional messages that were encrypted using the same key.

Known plaintext attacks can be used to break many types of encryption systems, including symmetric key ciphers and stream ciphers. In some cases, these attacks can be very effective and can even reveal the encryption key in a relatively short amount of time. As a result, it is important to use encryption algorithms that are resistant to known plaintext attacks and to protect the confidentiality of the plain text as much as possible.