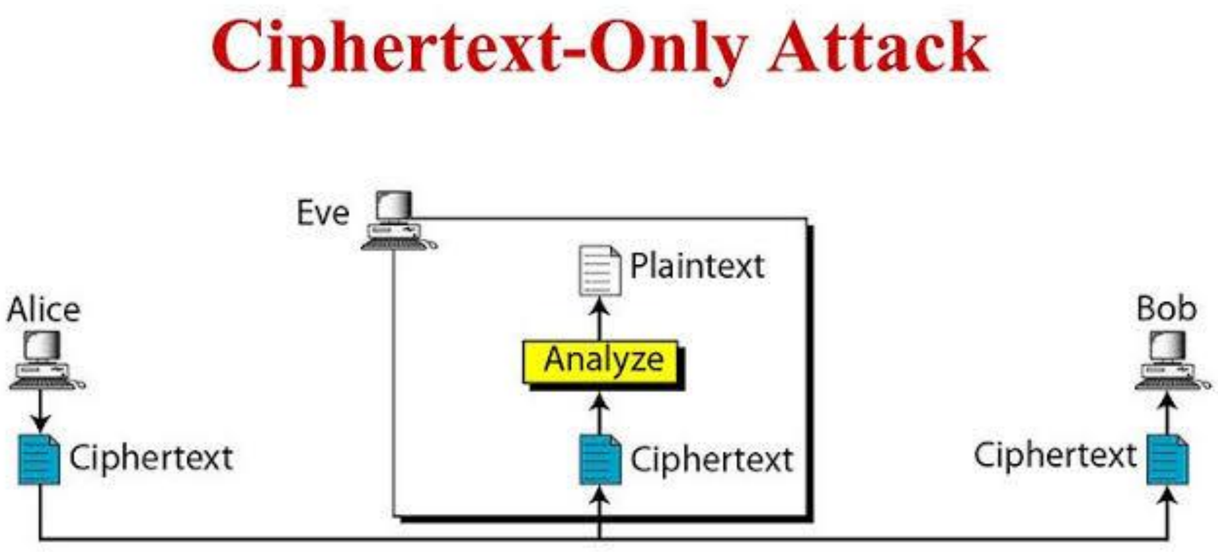
Practical List

Que10.

Cipher text only attack

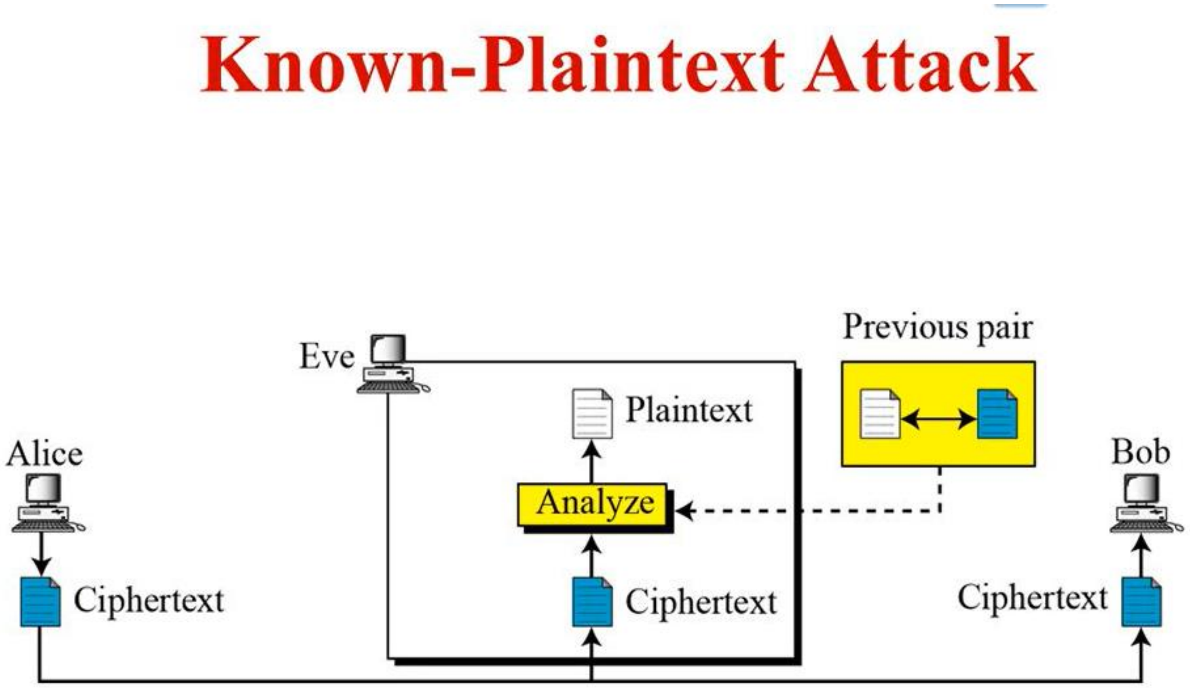
Ciphertext-only attack is a type of cryptanalytic attack in which the attacker has access only to the encrypted message, without any knowledge of the plaintext or the encryption key. The objective of the attack is to try to recover the original plaintext or the encryption key used to encrypt the message. Ciphertext-only attacks are often considered the most difficult type of attack to perform successfully, as the attacker has no information to use in their analysis other than the ciphertext.



An example of a ciphertext-only attack is a situation in which an attacker intercepts an encrypted message sent over the internet, without having access to the original plaintext or the encryption key. The attacker may then use various techniques, such as frequency analysis or brute force attacks, to try to break the encryption and recover the original message.

Known plaintext attack

Known plaintext attack is another type of cryptanalytic attack in which the attacker has access to both the plaintext and the corresponding ciphertext. The objective of the attack is to try to determine the encryption key used to encrypt the message, or to gain further knowledge about the encryption algorithm itself. Known plaintext attacks are often easier to perform than ciphertext-only attacks, as the attacker has some knowledge to work with.


Known-Plaintext Attack

An example of a known plaintext attack is a situation in which an attacker intercepts a message and knows both the original plaintext and the corresponding encrypted ciphertext. The attacker may then use this information to try to determine the encryption key used to encrypt the message, or to gain further insight into the encryption algorithm.