## Types of Attacks on Encrypted Messages:

| Type of Attack | Known to Cryptanalyst |
|---|---|
| 1. Ciphertext only (COA) | • Encryption algorithm<br>• Ciphertext to be decoded |
| 2. Known plaintext (KPA) | • Encryption algorithm<br>• Ciphertext to be decoded<br>• One or more plaintext-ciphertext pairs formed with the secret key |
| 3. Chosen plaintext (CPA) | • Encryption algorithm<br>• Ciphertext to be decoded<br>• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key |
| 4. Chosen ciphertext (CCA) | • Encryption algorithm<br>• Ciphertext to be decoded<br>• Purported ([illegible]) ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key |
| 5. Chosen text (CTA) | • Encryption algorithm<br>• Ciphertext to be decoded<br>• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key<br>• Purported ciphertext chosen by cryptanalyst together with its corresponding decrypted plaintext generated with the secret key |

• Note:- CTA < CCA < CPA < KPA < COA (according to hardness of attacks)
COA is the most difficult attack;
CTA is the most easy attack.

## Ciphertext-Only Attack (COA) (i)

In a ciphertext-only attack, the attacker (Eve) has access to only some ciphertext. She tries to find the corresponding key and the plaintext.

The assumption is that Eve knows the algorithm and can intercept the ciphertext.

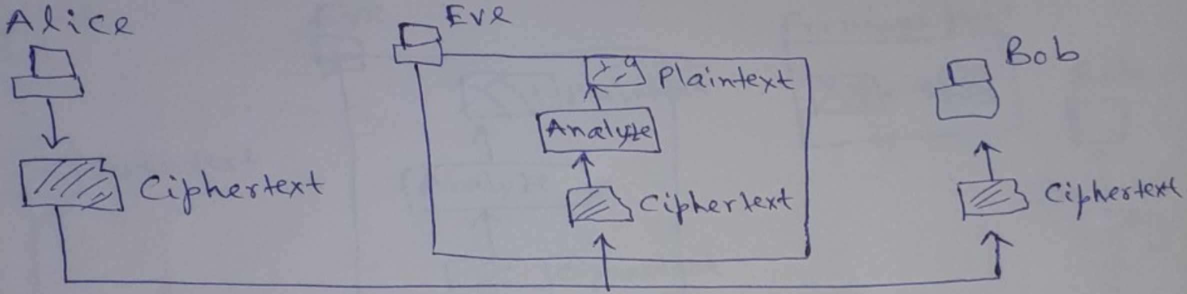
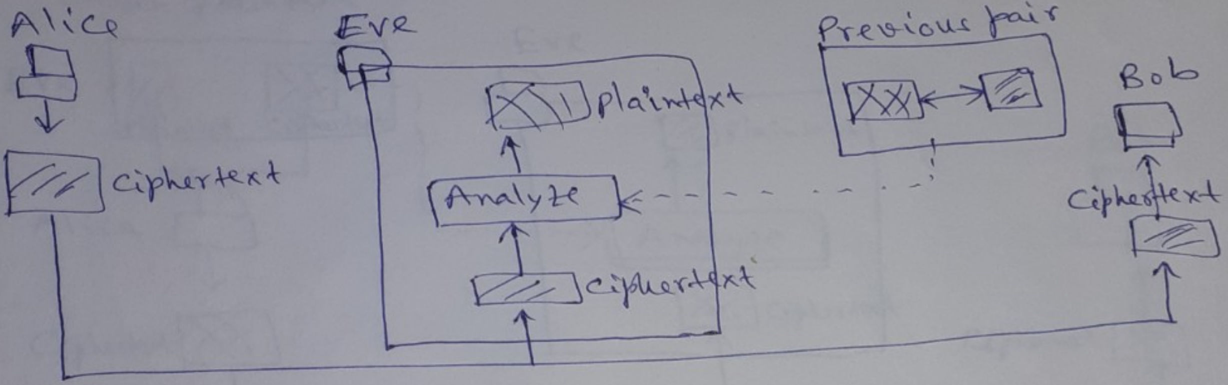


Fig. Ciphertext-only attack

## Known-Plaintext Attack (KPA)

(ii)

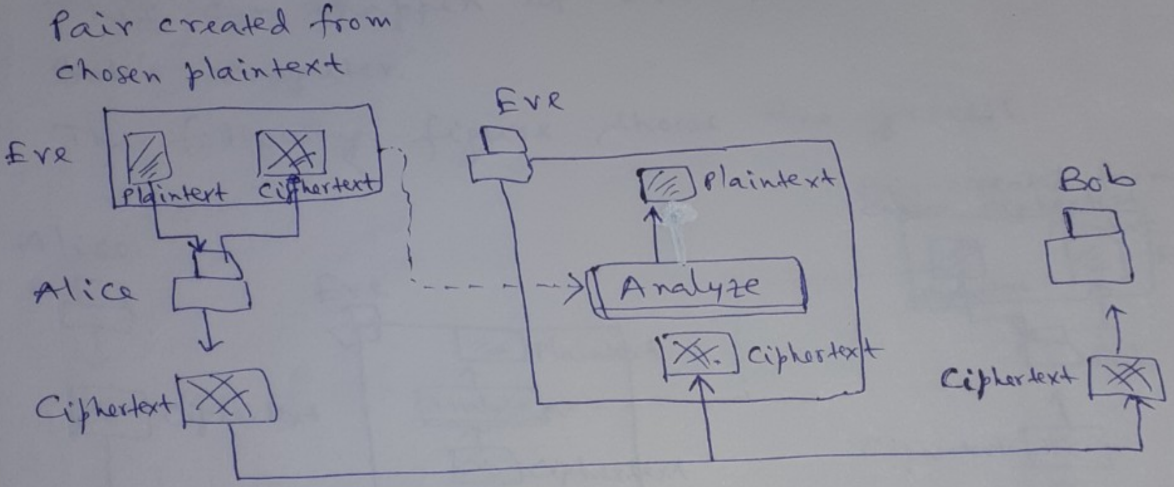
In a known-plaintext attack, Eve has access to some plaintext-ciphertext pairs in addition to the intercepted ciphertext that she wants to break, as shown in the following figure.



In this attack, the plaintext/ciphertext pairs have been collected earlier. For example, Alice has sent a secret message to Bob, but she has later made the contents of the message public. Eve has kept both the ciphertext and the plaintext to use them to break the next secret message from Alice to Bob, assuming that Alice has not changed her key.

## Chosen-plaintext Attack (CPA)

The chosen-plaintext attack is similar to the known-plaintext attack, but the plaintext/ciphertext pairs have been chosen by the attacker (Eve) herself. The following figure shows the process.



This situation can happen, for example, if Eve has access to Alice's computer. She can choose some plaintext and intercept the created ciphertext.

Of course, she does not have the key because the key is normally embedded in the software used by the sender.

This type of attack is much easier to implement, but it is much less likely to happen.

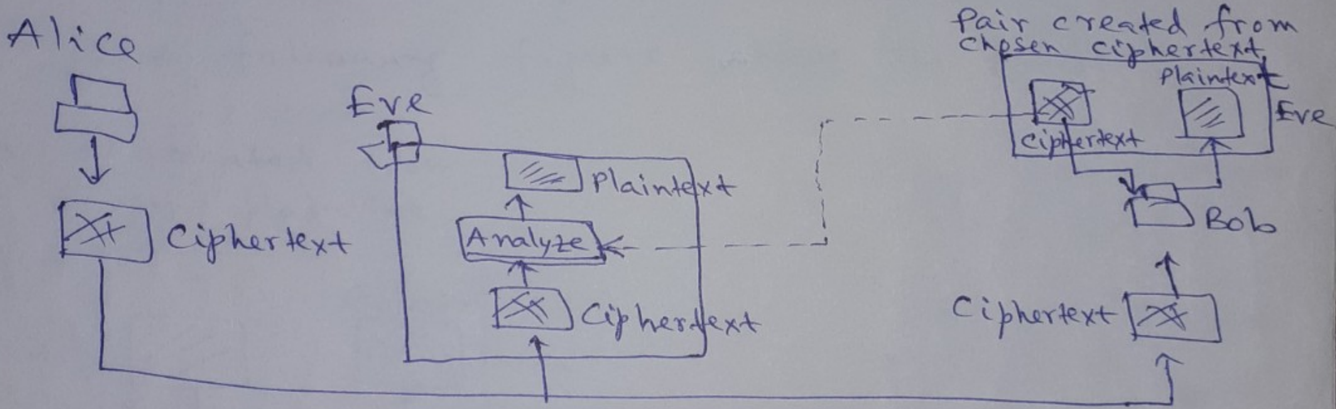
## Chosen-ciphertext Attack (CCA)

(iv)

The chosen-ciphertext attack is similar to the chosen-plaintext attack, except that Eve chooses some ciphertext and decrypts it to form a ciphertext/plaintext pair.

This can happen if Eve has access to Bob's computer.

The following figure shows the process.

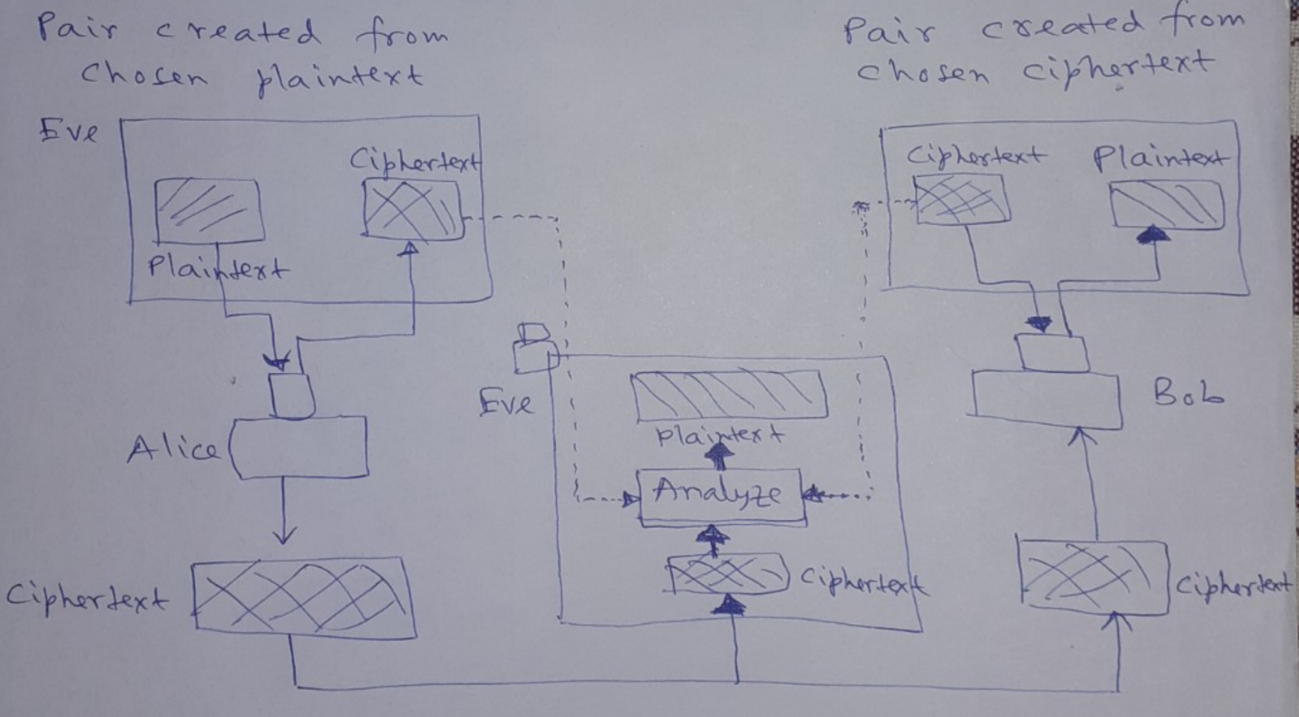


## Chosen-text Attack (CTA)

The chosentext attack is a combination of both the chosen-plaintext and chosen-ciphertext attacks. In this attack, an adversary, Eve chooses some plaintext and encrypts it to form a plaintext/ciphertext pair; and also chooses some ciphertext and decrypts it to form a ciphertext/plaintext pair.

This can happen if Eve has access to both Alice's computer and Bob's computer.

The following figure shows the process.



Pair created from chosen plaintext
Pair created from chosen ciphertext
Eve
Ciphertext
Plaintext
Alice
Ciphertext
Eve
Plaintext
Analyze
Ciphertext
Ciphertext
Plaintext
Bob
Ciphertext