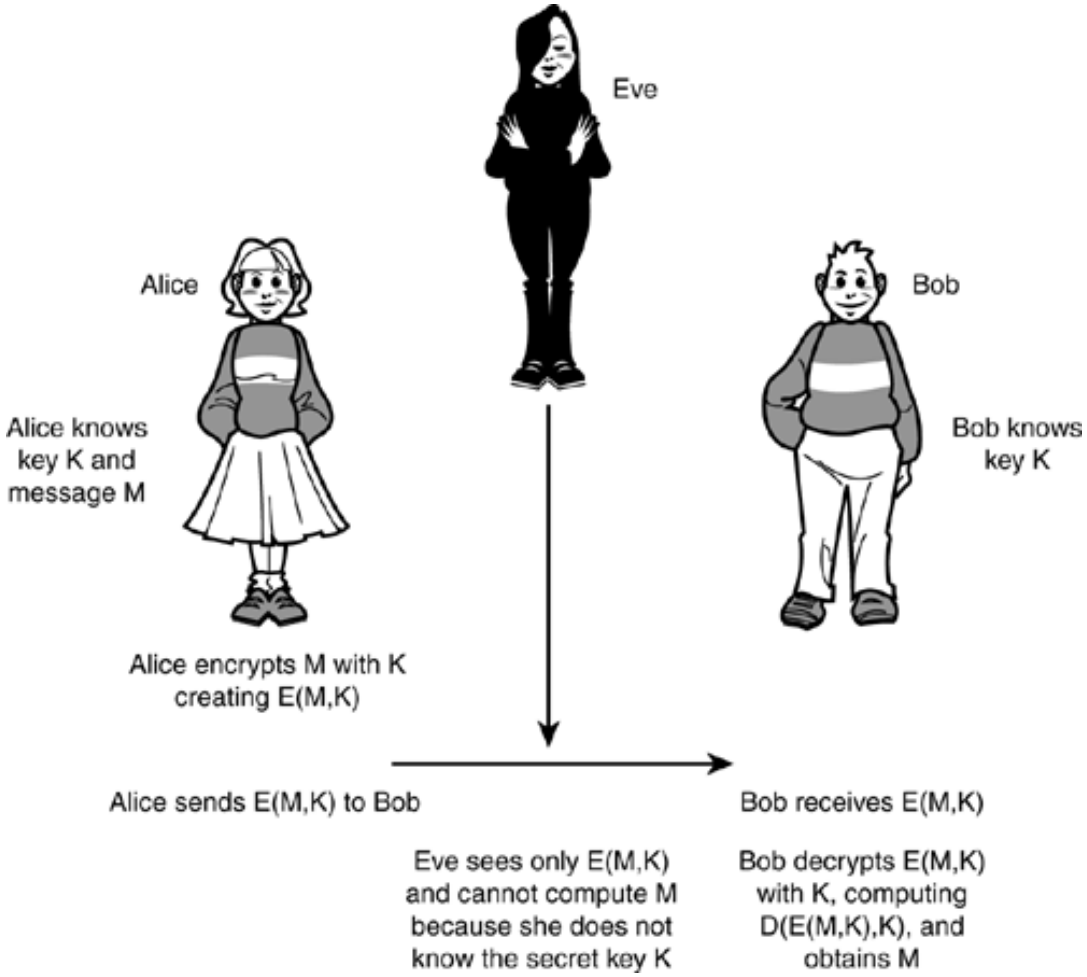
Basic Scenario of Cryptography

Basic Scenario of Cryptography

- Alice, who wants to say something privately to Bob
- Bob, who wants to hear from Alice
- Eve, the person who is trying to eavesdrop on their conversation.
  Eve's goal:
  - Read M
  - Get the Key Alice is using, and real all messages encrypted using that key
  - Modify the content of the message in such a way that Bob will think Alice sent the altered message.
  - Impersonate Alice and communicate with Bob who thinks he is communicating with Alice.

Passive

Active



(https://flylib.com/books/en/1.581.1.188/1/)

Terminologies of Cryptography

- **Cryptography: the art of secret writing**
  - The art of mangling information into apparent unintelligibility in a manner that allows a secret method of unmangling.
- **Related terminologies**
  - Cryptology: The study of communication over non-secure channels, and related problems
  - Cryptography: The process of designing systems that achieve secure communications.
  - Cryptanalysis: Breaking such systems. (The techniques used to recover the secret information hidden in cryptographic systems)
  - Plaintext: message to be sent, in readable form
  - Ciphertext: message in coded form, unreadable without special information such as a key
  - Encrypt: turn plaintext into ciphertext
  - Decrypt: turn ciphertext back into plaintext

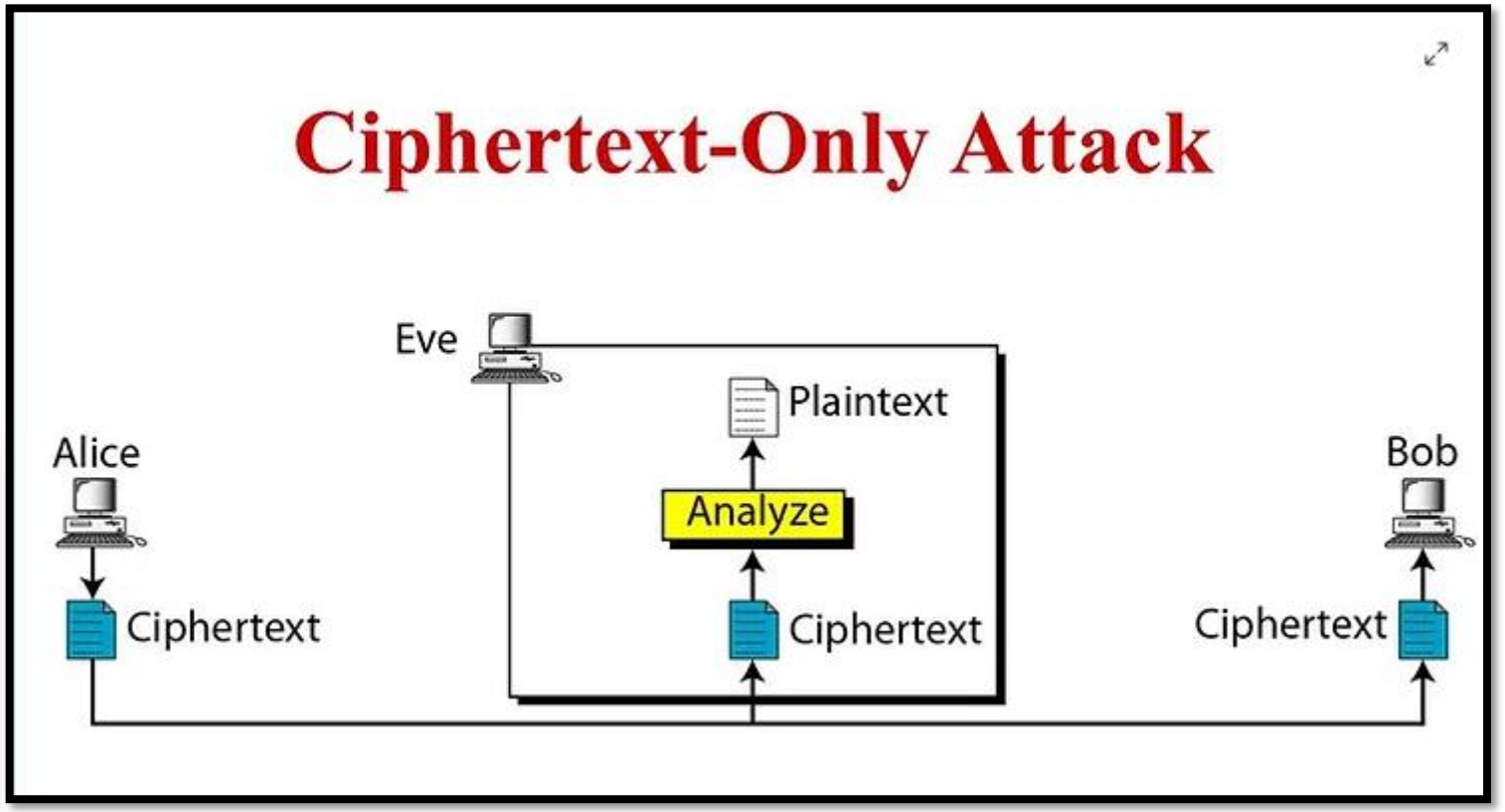
Cryptosystem attacks

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext attack

Ciphertext-only attack - Example

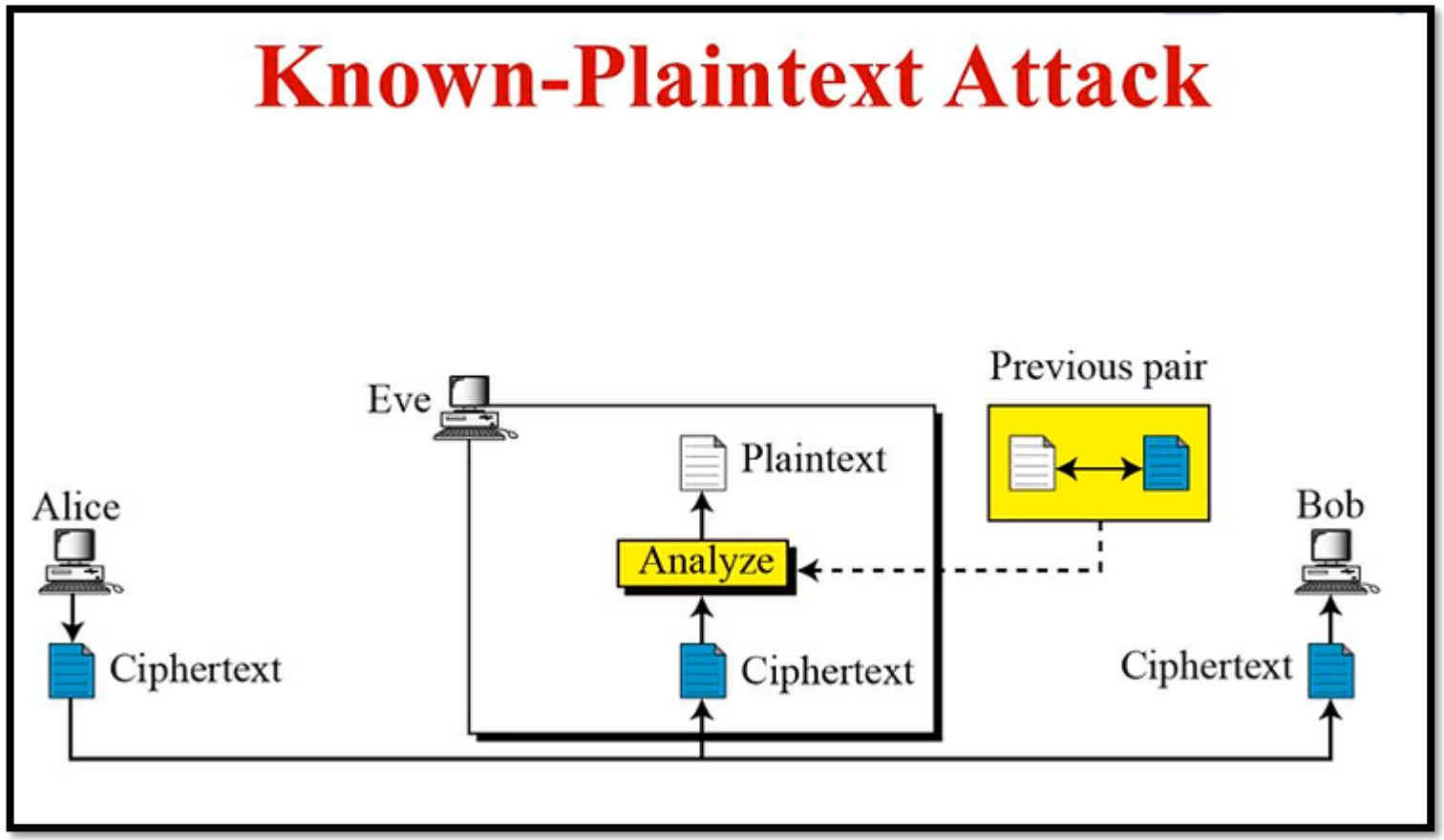
In this attack on the encryption, attacker/cryptanalyst can only observe the ciphertext.

```
hQIMAw3Jn/nLK/38ARAAsSXLDhCtzUYKMptNxZImJXwhhIRm3QxfuyHjJ93ASylE
e+6ABkuyFLJhiKryxp/JmS/alMPfF7hx2aTgovagaPzTwTV1jo6If2mhdCl6keed
1Iz7C0f6jHIqq9d8g0bWDyvELEipn5LNDTX3Xp2Csx5ojRB2wckrUtll1Xyj8G0H
4DQUYbINRmJVulJJC/acGvgOze66pHuRgSCxxHDscefjXenh/XejSYTo7aMi+Es7
DCcD49zH6ZLDQN6BlN9q2oFI8QIhQ2y1QJbat1dWi/4yYWlKZcLKRSm8eo/gNCdL
h9MncXBBSfgbvbu67CDZ9GO5geZOn3LzQOpJ8hrZq/6K/uMcUKeZjW3RCo0T754f
E5zYe1wUgtwS/lmQ2w5PQF/89bpshtDSYuL1fZgzrsE6DwophuCri5zwCGbEKlsI
g6REIETFbZ2aCL4N2pZVunCIEuoP0zgEB6+M9egdpyxMsMqEBVg3AH7Sa1AtEguP
T/MCxI0bZHCUhPupEKT8slbSrDNxTWMUXQt3XpL0bGCCrDMKLSoWYfDiNnRkFbWK
iiqw9hx4Q9CJg7xX7JRnVgwOeREiFnMYSbFlvPSxEOu6FdBYhdqSefKin4Wnkmdw
qrSl8fjIW/kZ2v72uz0buEKkY9ubBox76yjlRo9KUQMs3em03kc64959gTDiZ0qF
AgwDrosDPQ2BeYQBD/9H5VKFw0an5j5MX1JpOSBAqNGKWq2bcEFnwJfk0DDlhyHD
owHiG7gDowCS+5y/pf56v36HkzpJZATKqoRyKVxmQOxU9l3YnPc5fw8iFhxlrfcG
ywzkJh/BRDQ/uy5fhGc/PbSm6iLv/SkkWTK8PSUD+g1yZyK0W7WkMh9QYS2OE7lQ
qbwpNiy57reWkUWCoE4QmKqqpe7NXXM0eLT9l2D0hG2lthyvTvspkpxszl8+HMJv
M2LMcY2FmmZWAJSdxsQSq9NQdyvCJX2D8oa89WQyXmp7mPXL7BQfoQNPndmn6Obi
0EQojoeMRNh14XNhMjPjxW7m34rH2gtvdN3Dg8iFrtocoVJqXqU3N+9T2sNe/bS8
```



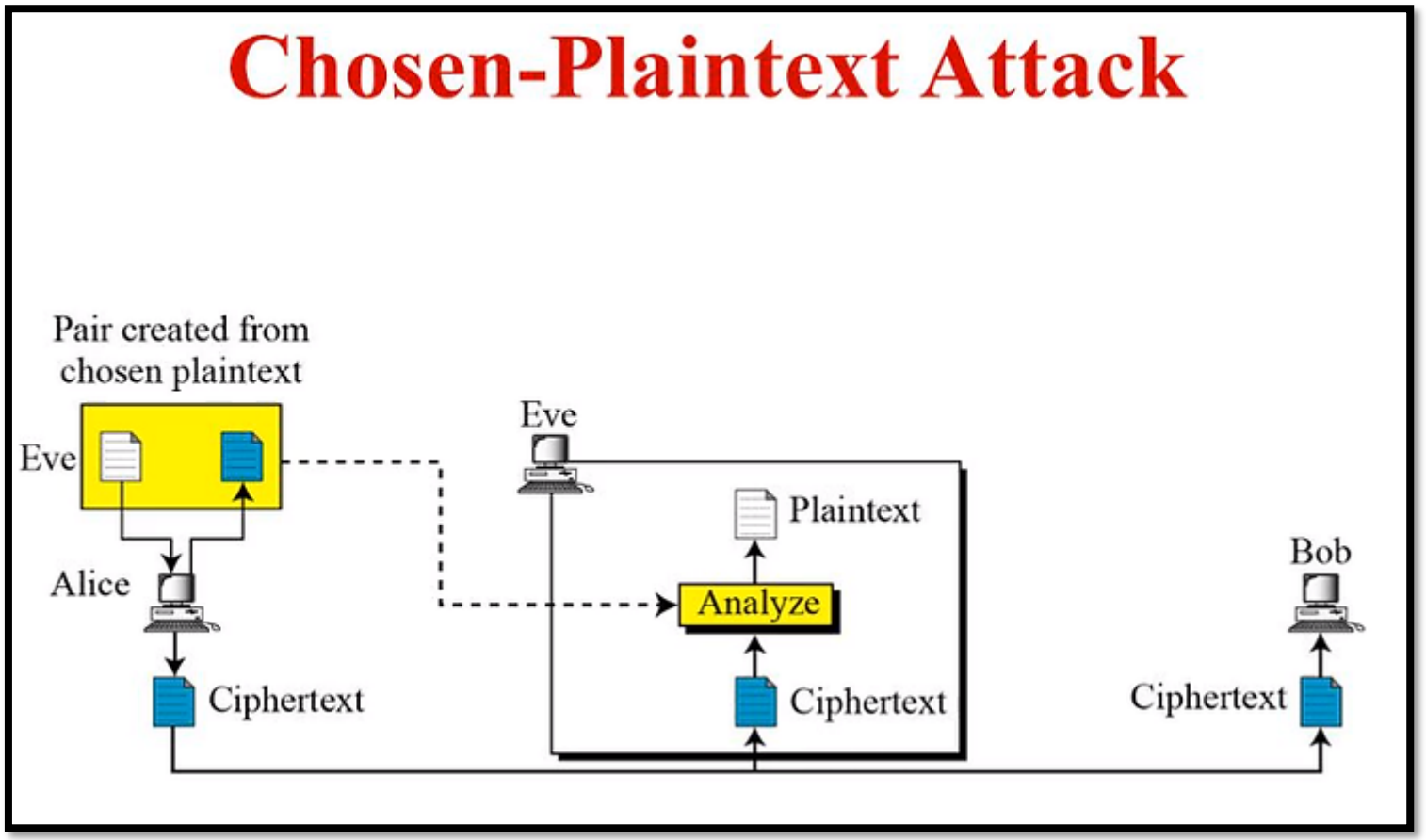
Known-plaintext attack - Example

- In this attack, the attacker/cryptanalysts know the plaintext that generates the ciphertext. They can't select the plaintext, but they can observe plaintext-ciphertext pairs.
- This attack has a significantly better chance of success than COA.



Chosen-plaintext attack - Example

- In this attack, the cryptanalyst can select or choose the plaintext that is sent through the encryption algorithm and observe the ciphertext that it generates.
- An active model where the attacker actually gets to chose the plaintext and do the encryption.



Chosen-ciphertext attack - Example

In this attack, the attacker can both encrypt and decrypt. This means that they can select plaintext, encrypt it, observe the ciphertext and then reverse the entire process.