جامعة الحمدانية /كلية التربية

قسم علوم الحاسوب

Fourth Class

Data Security

أستاذ المادة:

م. سماح فخري عزيز

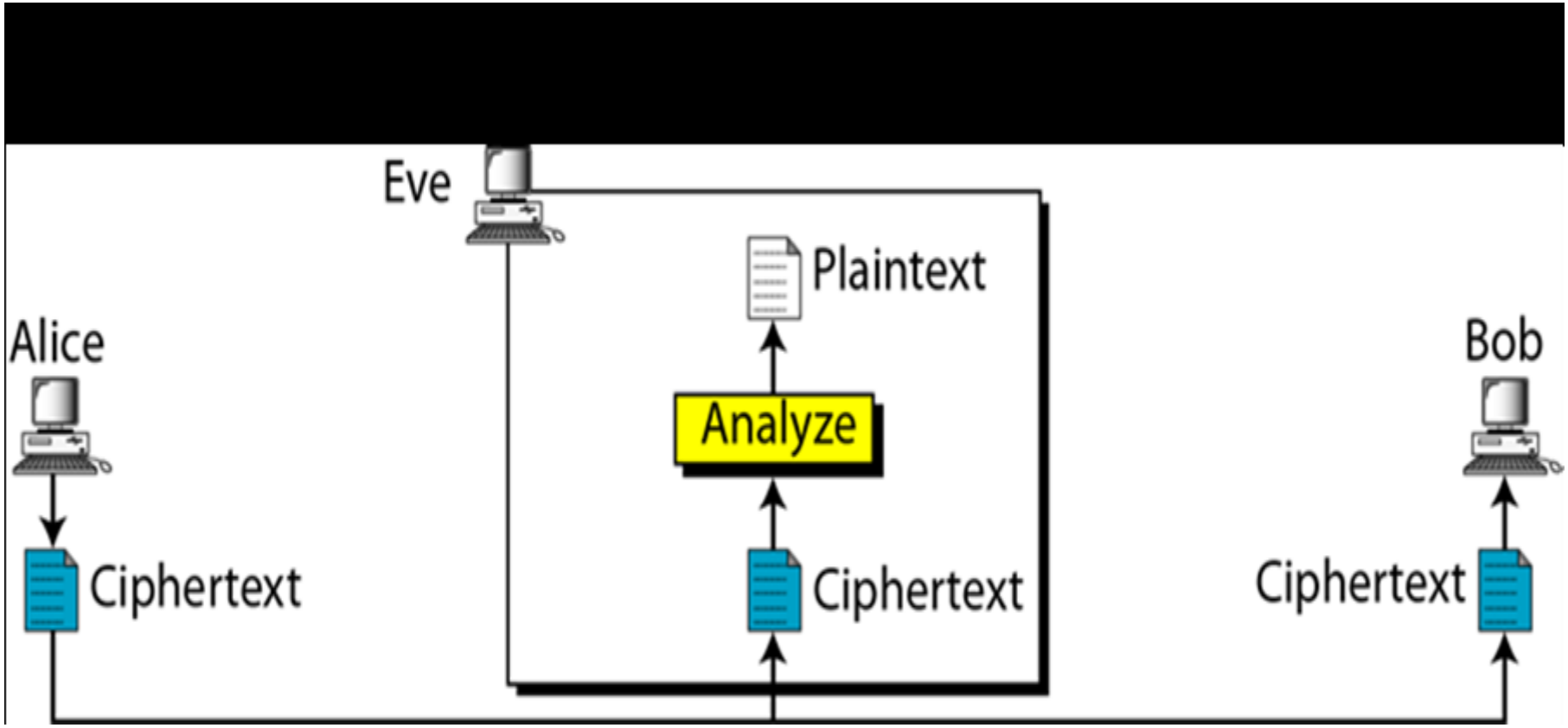
- **Attacks on Cryptosystems**

Cryptanalysis and Attacks on Cryptosystems

- There are many cryptanalytic techniques. Some of the more important ones for a system implementer are

- **Ciphertext-only attack** (Only know algorithm / ciphertext, statistical, can identify plaintext): This is the situation where the attacker does not know anything about the contents of the message, and must work from ciphertext only. It is very hard.

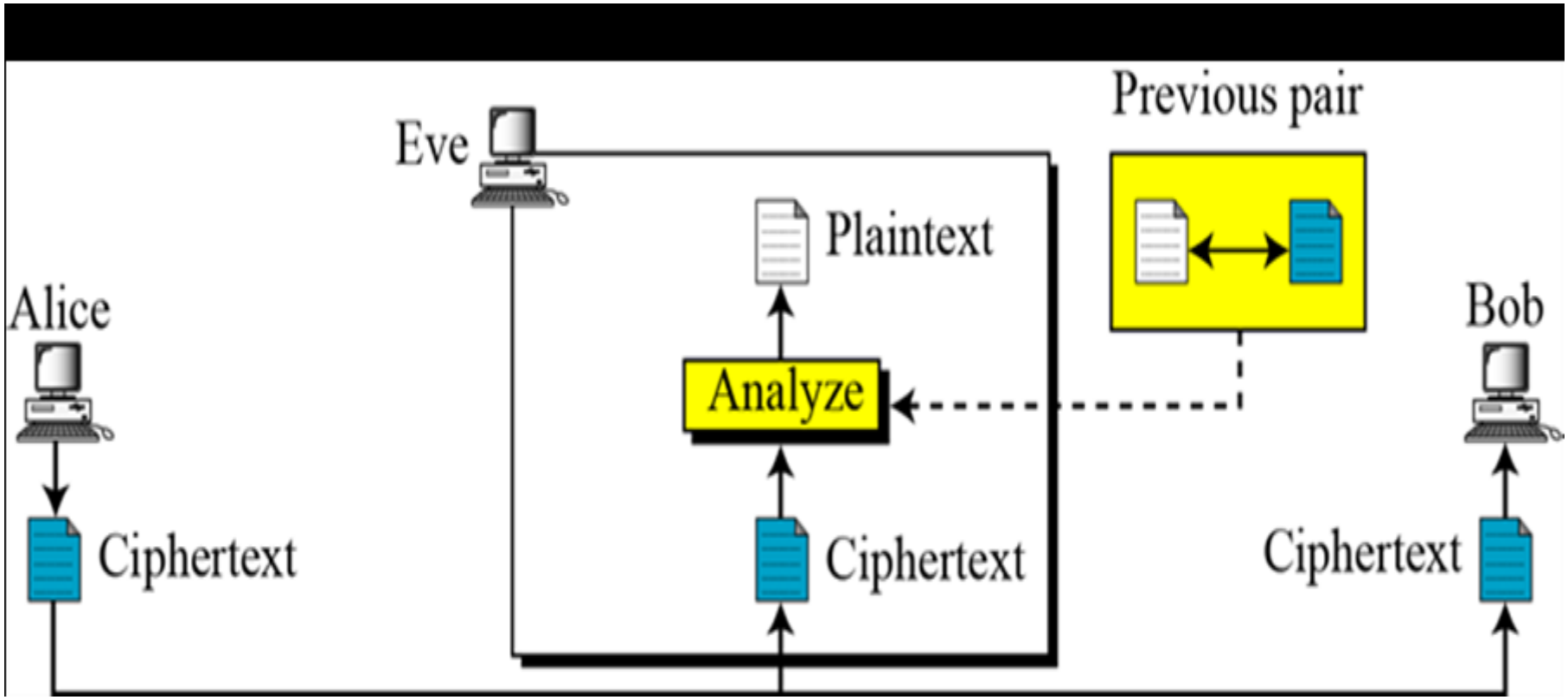
- **Ciphertext-only attack**



Known-plaintext attack

- ***Known-plaintext attack*** *(know/suspect plaintext & ciphertext to attack cipher): The attacker knows or can guess the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext blocks using this information. This may be done by determining the key used to encrypt the data, or via some shortcut*

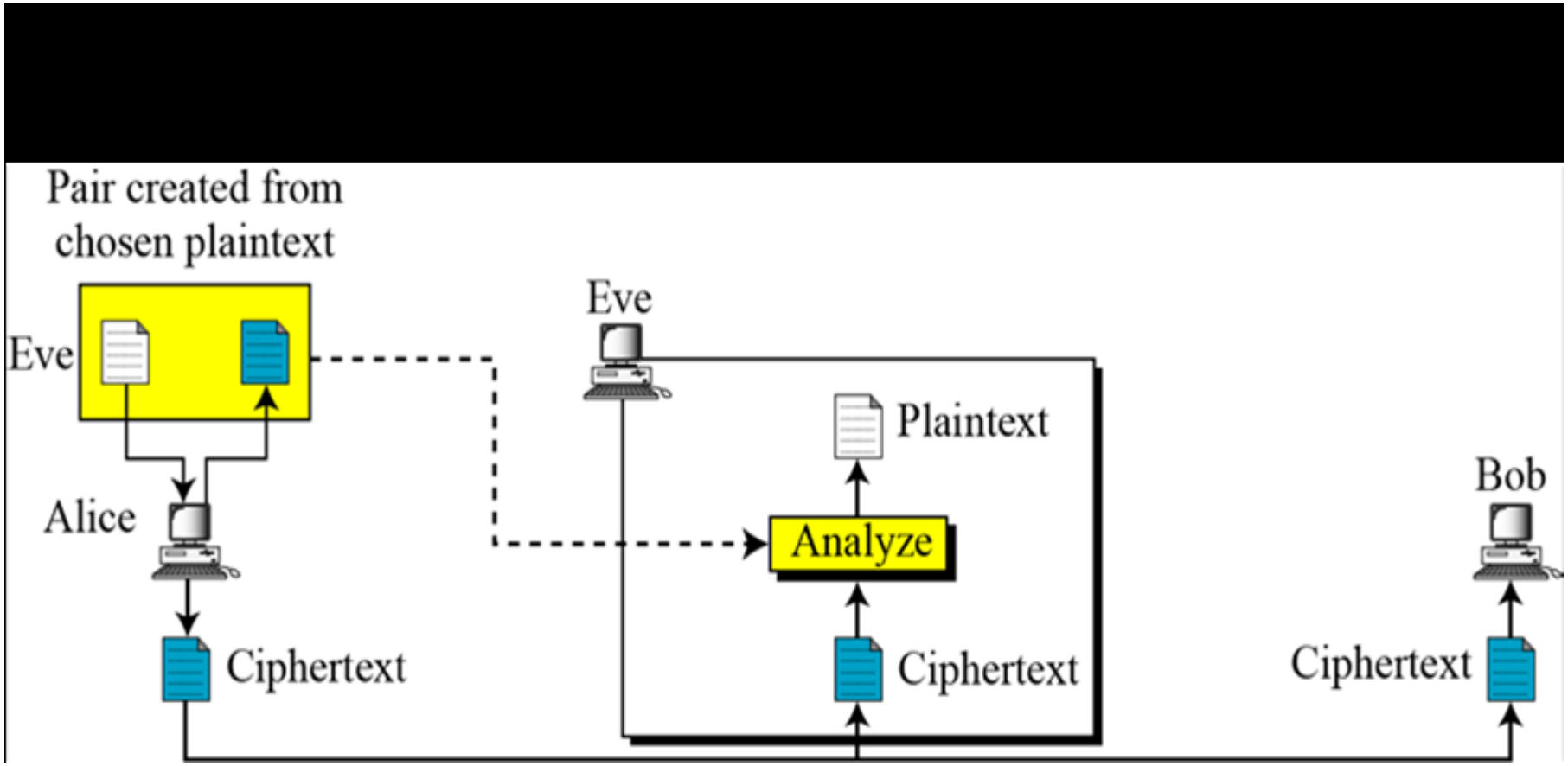
- **Known-plaintext attack**



Chosen-plaintext attack

- ***Chosen-plaintext attack*** *(selects plaintext and obtain ciphertext to attack cipher): The attacker is able to have any text he likes encrypted with the unknown key. The task is to determine the key used for encryption.*

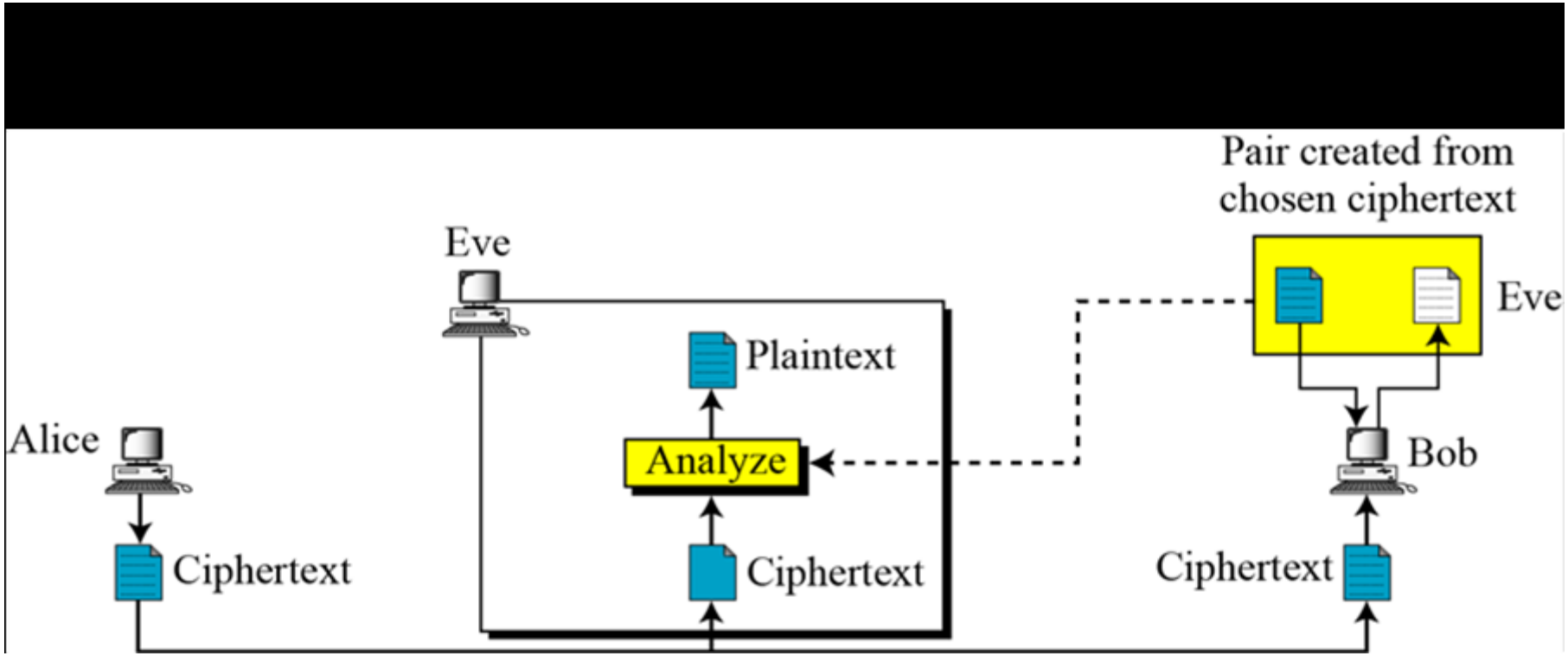
- **Chosen-plaintext attack**



Chosen Ciphertext Attacks

- ***Chosen Ciphertext Attacks*** *(select ciphertext and obtain plaintext to attack cipher)**:** Attacker obtains the decryption of any ciphertext of its choice (under the key being attacked)*

- **Chosen Ciphertext Attacks**



Thank you