الجامعة المستنصرية /كلية التربية / قسم علوم الحاسبات

4th Class
Computers & Data Security
أمنية الحاسوب والبيانات

أستاذ المادة

أ.م . د . اخلاص عباس البحراني

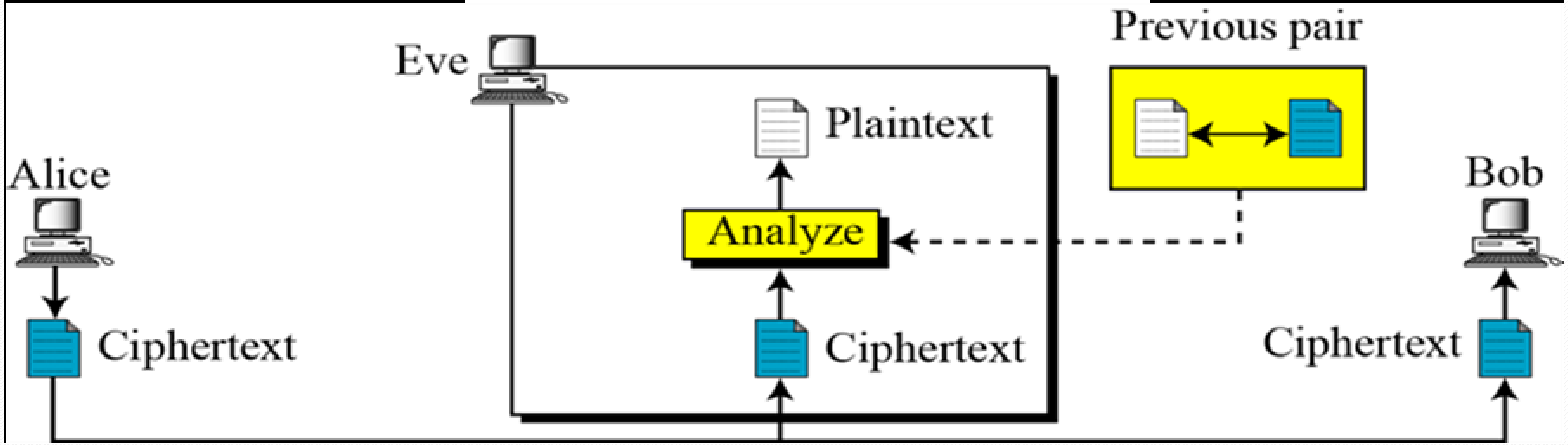
Cryptanalysis and Attacks on Cryptosystems

- 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
Eve
Plaintext
Alice
Bob
Analyze
Ciphertext
Ciphertext
Ciphertext

- **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** (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
Pair created from chosen plaintext
Eve
Alice
Ciphertext
Eve
Plaintext
Analyze
Ciphertext
Bob
Ciphertext

- **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
Pair created from chosen ciphertext
Eve
Eve
Plaintext
Alice
Analyze
Bob
Ciphertext
Ciphertext
Ciphertext

Chapter three
Mathematics

- **Modular Arithmetic**
  - several important cryptosystems make use of modular arithmetic. This is when the answer to a calculation is always in the range 0 – *m* where m is the **modulus**.
  - (a mod n) means the remainder when a is divided by n.
  - a mod n = r
  - a div n=q
  - a = qn + r
  - r = a – q * n

Example :- if a=13 and n=5, find q and r.

q=13 div 5=2 and r=13-2 *5=3 which is equivalent to (13 mod 5)

Example :- find (-13 mod 5).

This can be found by find the number (b) where 5*b >13 then let b=3 and 5*3=15 which is less than 13 so

-13 mod 5=5*3-13=2