جامعة الحمدانية /كلية التربية
قسم علوم الحاسوب
Fourth Class

Data Security

أستاذة المادة:

م. سماح فخري عزيز

- **Symmetric and Public Key Systems**

CONTENTS

- **Symmetric-key**
- **Public-Key Cryptography**
- **Public-Key Characteristics**
- **Public-Key Applications**
- **Cryptography, Cryptanalysis**
- **Attacks on Cryptosystems**

Symmetric-key or (or secret-key)

- ***Symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key)***

Symmetric-key or (or secret-key)

- **two main types:**

- **stream ciphers** – operate on individual characters of the plaintext

- **block ciphers** – process the plaintext in larger blocks of characters

Private Key Encryption (Symmetric)

Public-Key Cryptography

- public-key/two-key/asymmetric cryptography involves the use of two keys:

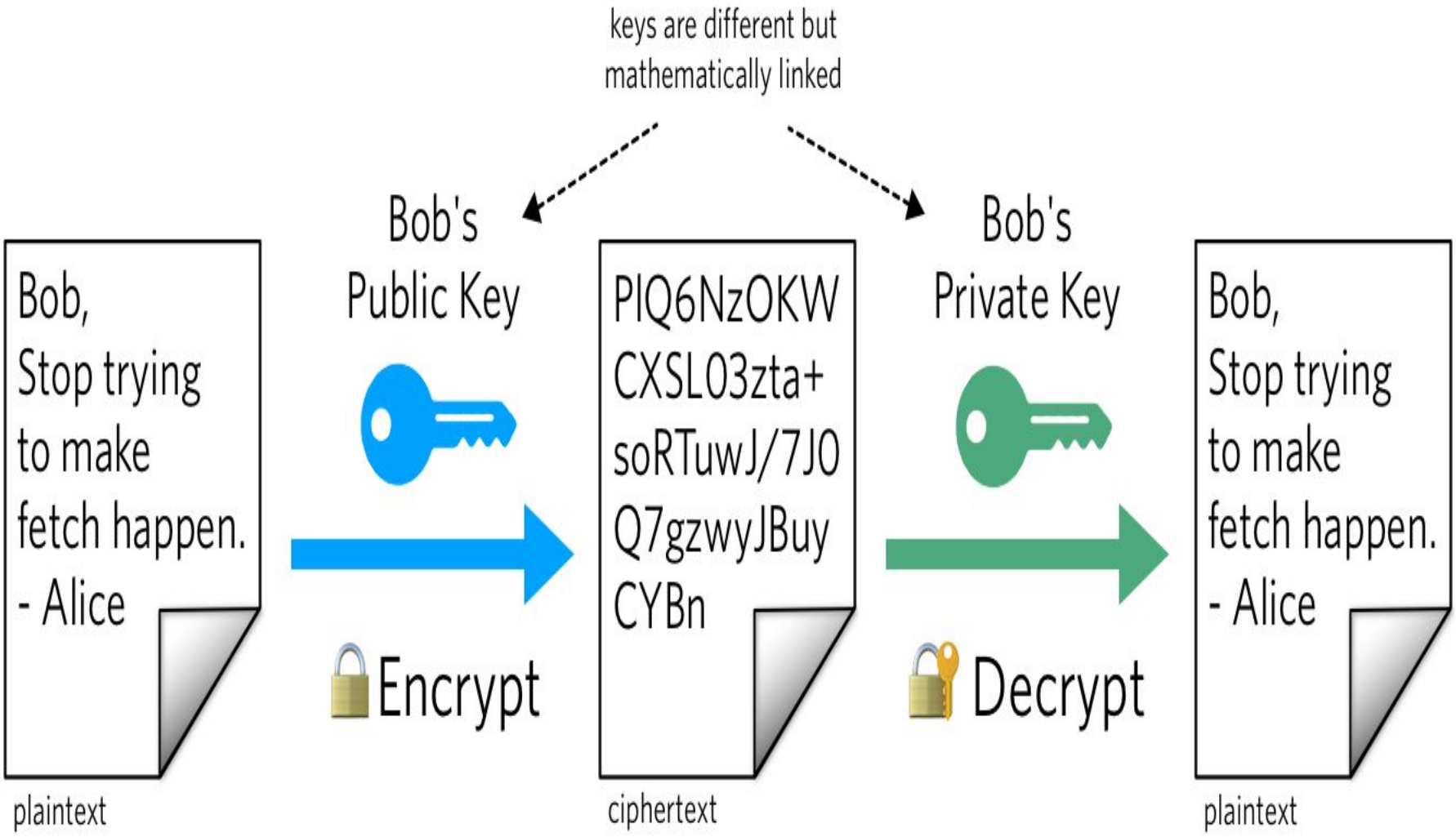
- **a public-key**, which may be known by anybody, and can be used to encrypt messages, and verify signatures

- **a private-key**, known only to the recipient, used to decrypt messages, and sign (create) signatures

Public-Key

is asymmetric because those who encrypt messages or verify signatures cannot decrypt messages or create signatures

Public Key Cryptography



Public-Key Characteristics

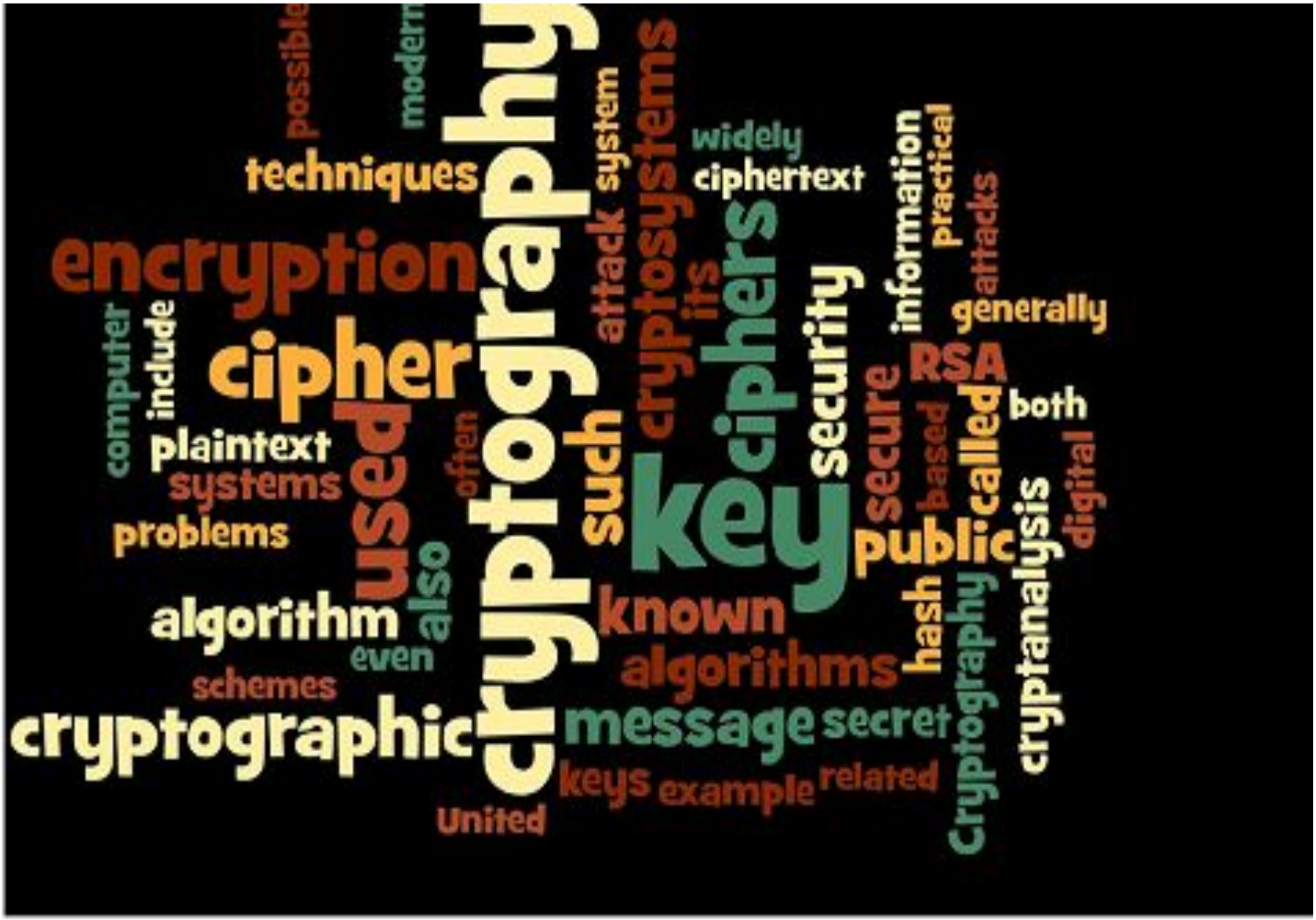
- it is computationally infeasible to find decryption key knowing only algorithm & encryption key

- it is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known

- either of the two related keys can be used for encryption, with the other used for decryption (for some algorithms)

Public-Key Applications

- can classify uses into 3 categories:
- ***encryption/decryption (provide secrecy)***
- ***digital signatures (provide authentication)***
- ***key exchange (of session keys)***


cryptography
encryption
cipher
key
used
ciphers
cryptosystems
techniques
ciphertext
widely
information
practical
attacks
generally
security
RSA
public
secure
called
both
digital
cryptanalysis
Cryptography
hash
algorithms
known
algorithm
message
secret
cryptographic
plaintext
systems
problems
computer
include
possible
modern
attack
system
its
such
often
also
even
schemes
keys
example
related
United

Cryptography, Cryptanalysis, Cryptology

- **Cryptography** is the art or science of keeping messages secret.

- **Cryptanalysis** is the art of **breaking** ciphers, i.e. retrieving the plaintext without knowing the proper key.

- **Cryptology** is the branch of mathematics that studies the mathematical foundations of cryptographic methods.

- People who do cryptography are **cryptographers**, and practitioners of cryptanalysis are **cryptanalysts**.

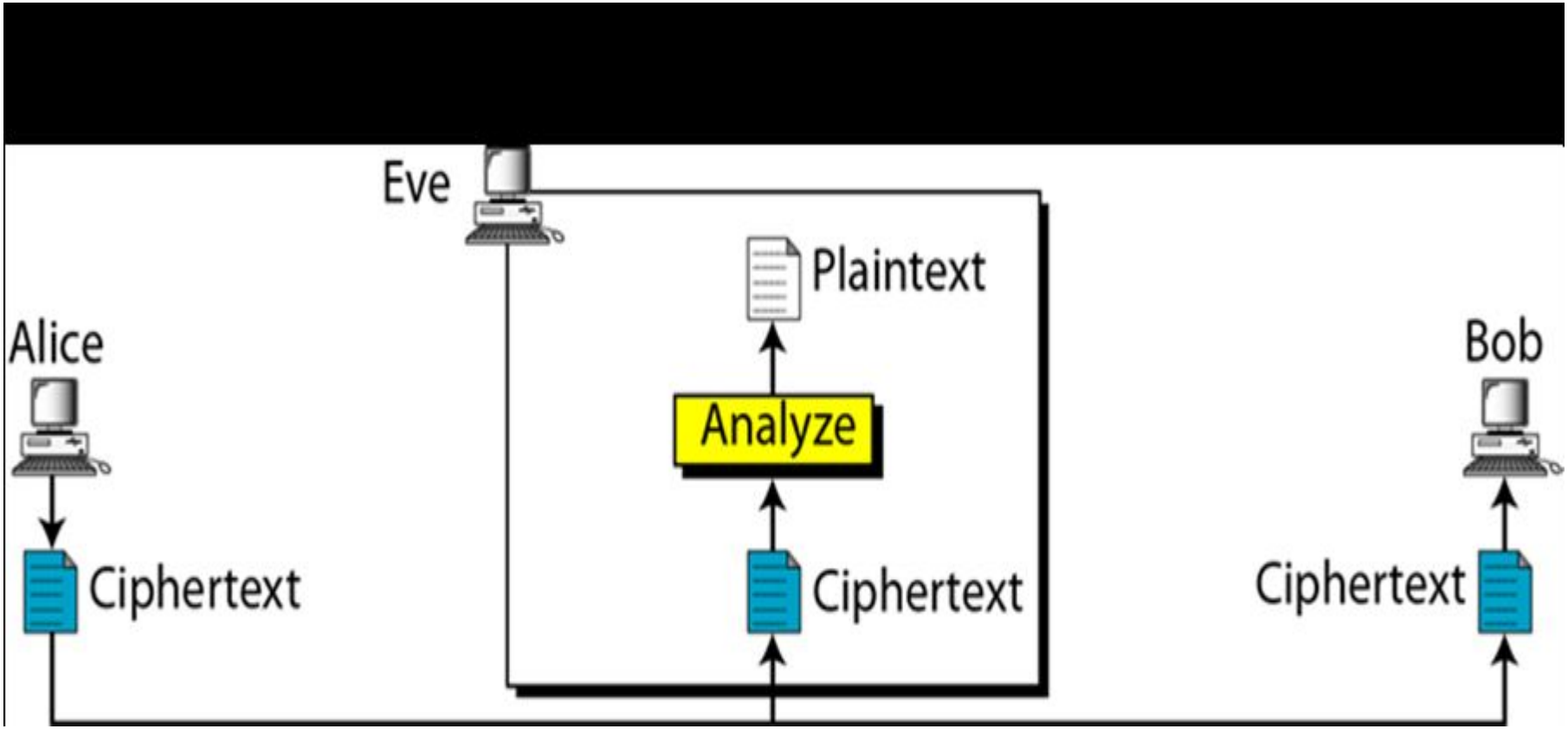
- **Cryptography** deals with all aspects of secure messaging, authentication, digital signatures, electronic money, and other applications.

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.

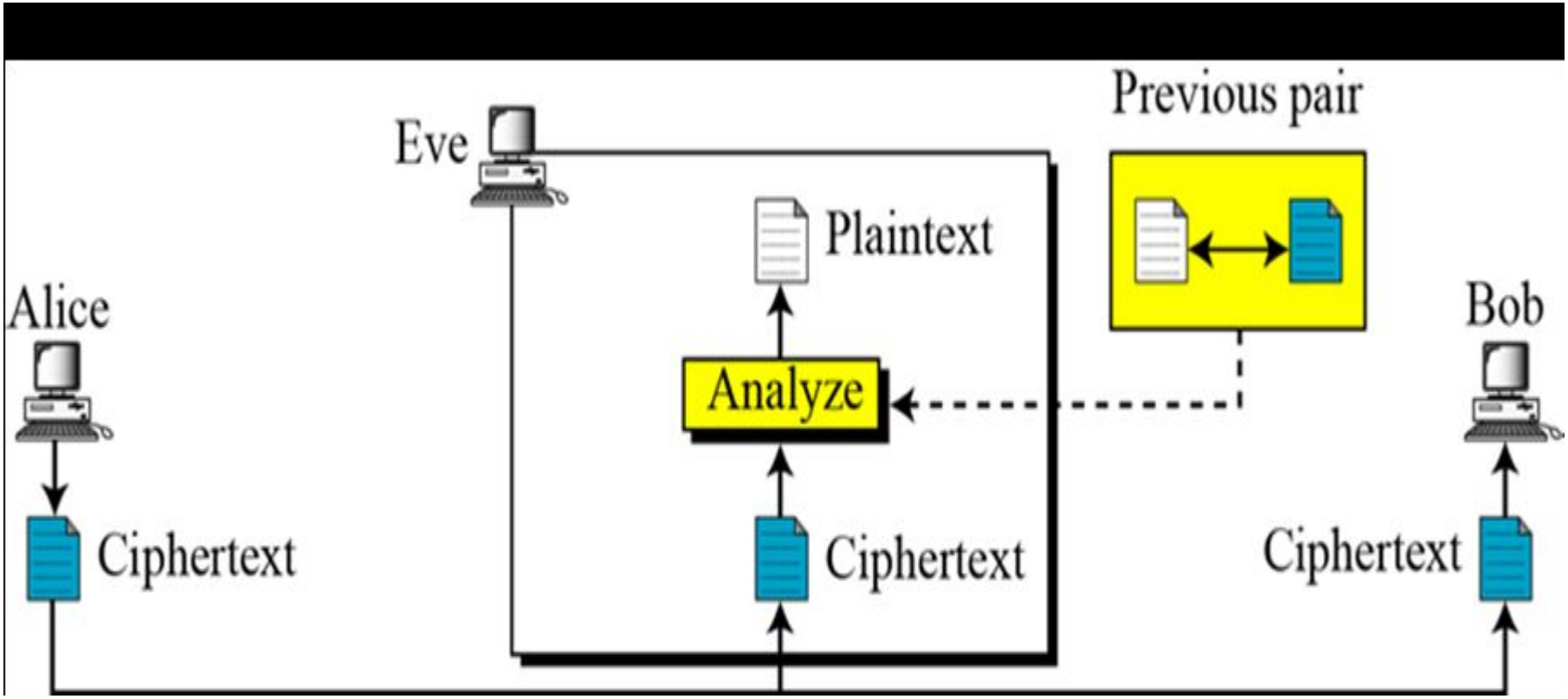
- **Ciphertext-only attack**



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*

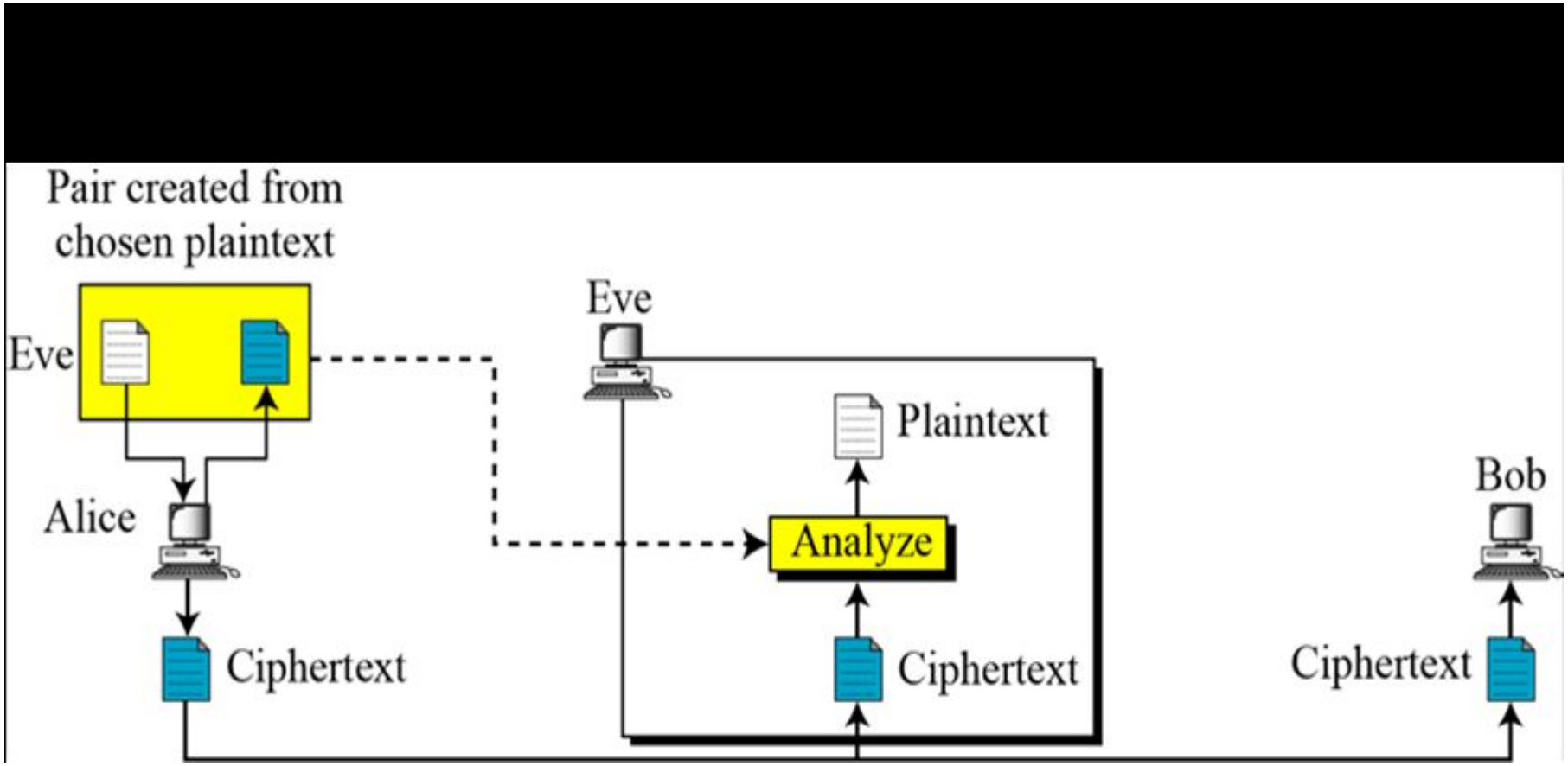
- **Known-plaintext attack**



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.*

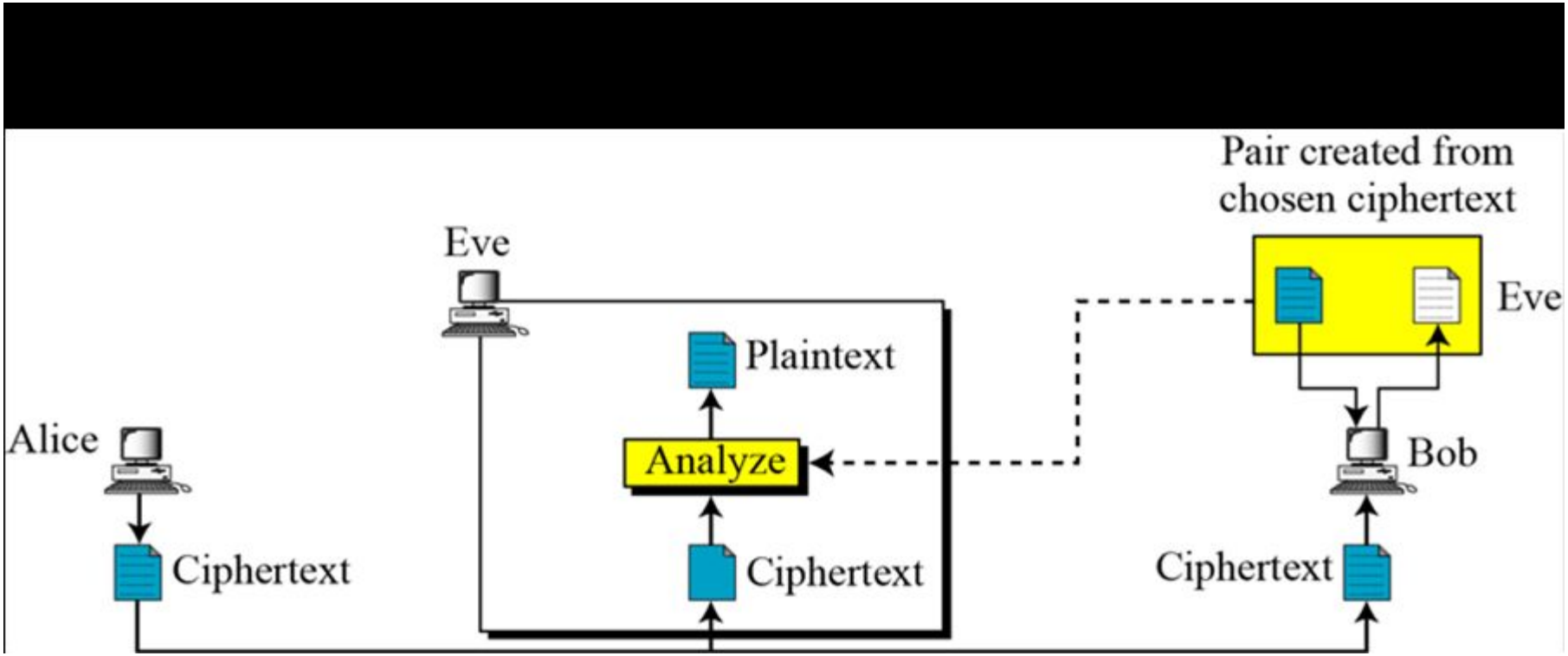
- **Chosen-plaintext attack**



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