Chapter 2
Terminology and Background

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

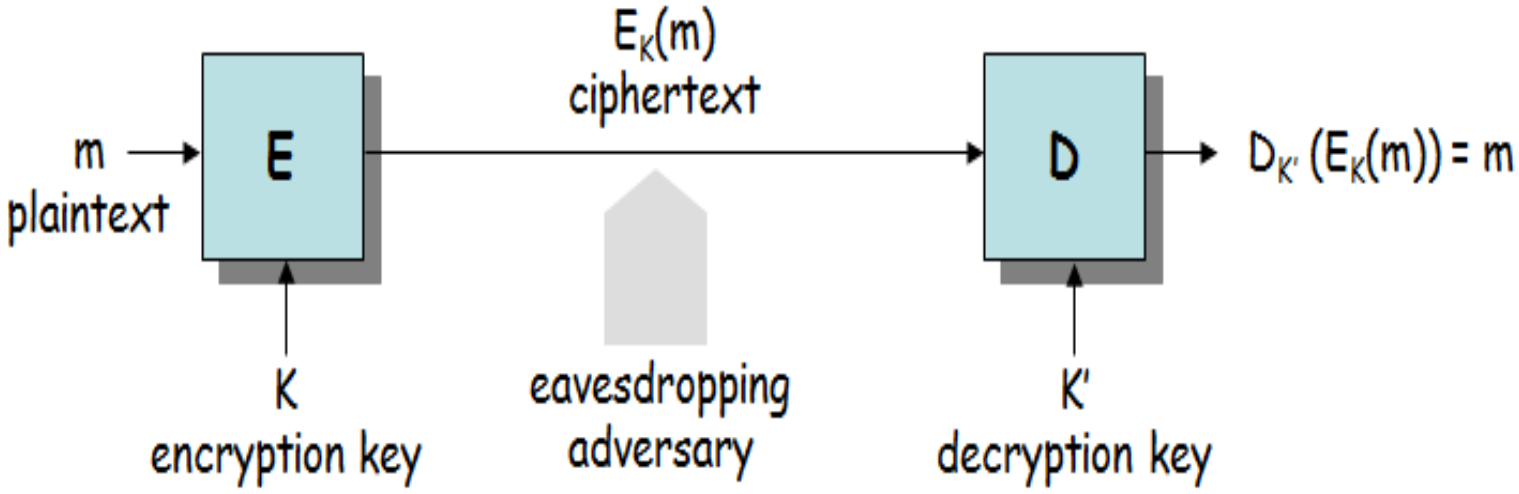
Components of a Cryptosystem

The various components of a basic cryptosystem are as follows : -

- **Plaintext.** It is the data to be protected during transmission.
- **Encryption Algorithm.** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
- **Ciphertext.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
- **Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- **Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.
- For a given cryptosystem, a collection of all possible decryption keys is called a **key space**.

Basic Cryptographic Algorithms

- A **cipher** is the method of encryption and decryption.
- Some cryptographic methods rely on the secrecy of the algorithms. **Keyless Cipher** is a cipher that does not require the use of a key.
- All modern algorithms use a **key** to control encryption and decryption; a message can be decrypted only if the key matches the encryption key.
- The key used for decryption can be different from the encryption key, but for most algorithms they are the same.



Classical model of encryption

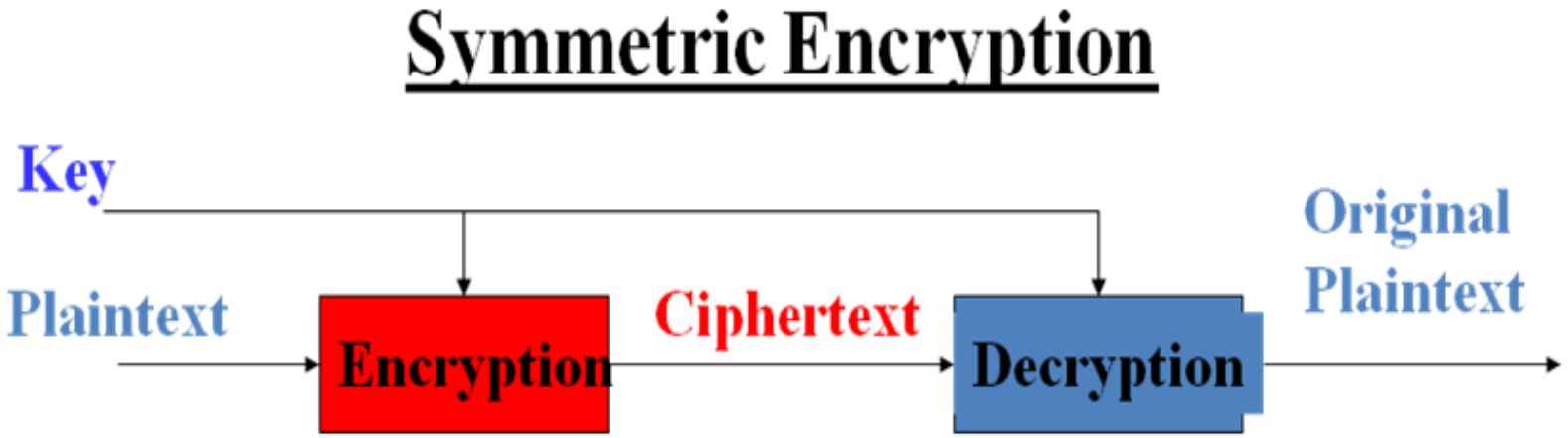
Basic classification of encryption key-based algorithms

1. **Symmetric-key or (or secret-key) encryption algorithm.**

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

two main types: –

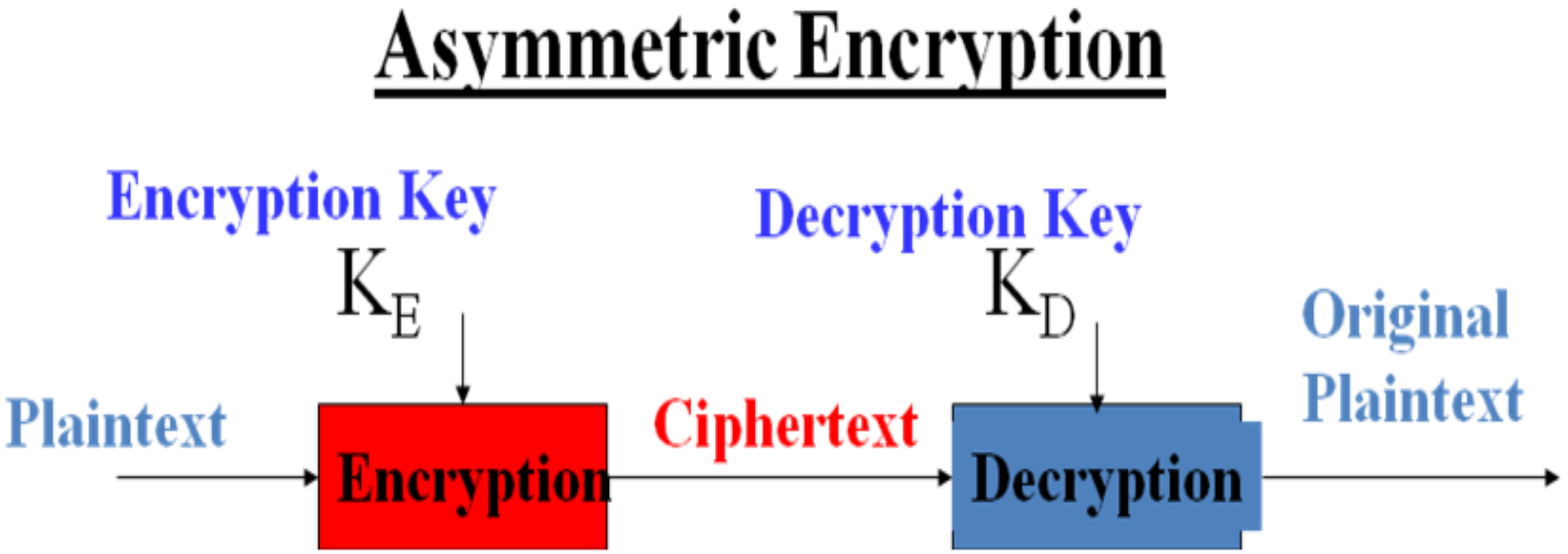
- **stream ciphers** – operate on individual characters of the plaintext
- **block ciphers** – process the plaintext in larger blocks of characters



2. **Asymmetric (or public-key) encryption algorithms.**

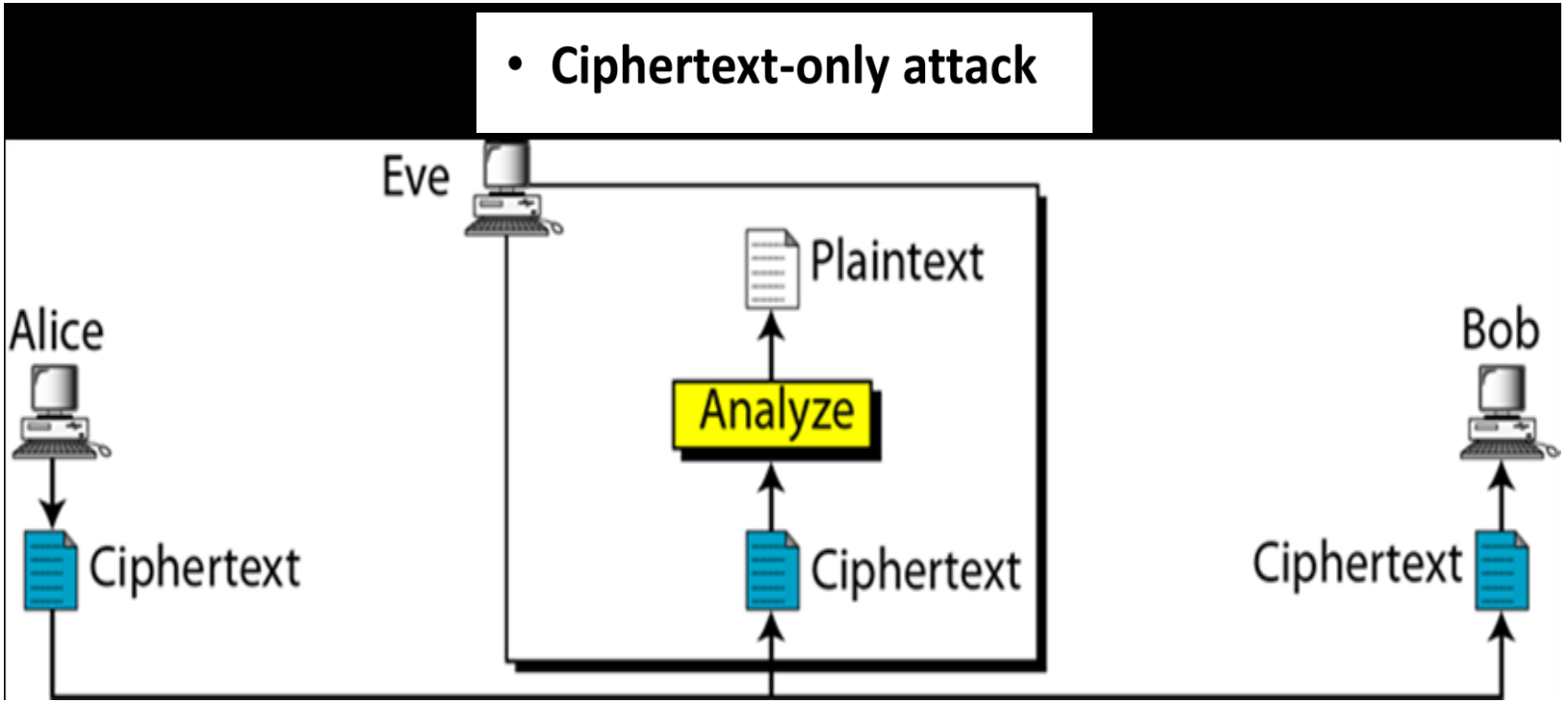
- algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key.
- permit the encryption key to be public (it can even be published in a newspaper), allowing anyone to encrypt with the key, whereas only the proper recipient (who knows the decryption key) can decrypt the message. The encryption key is also called the **public key** and the

s



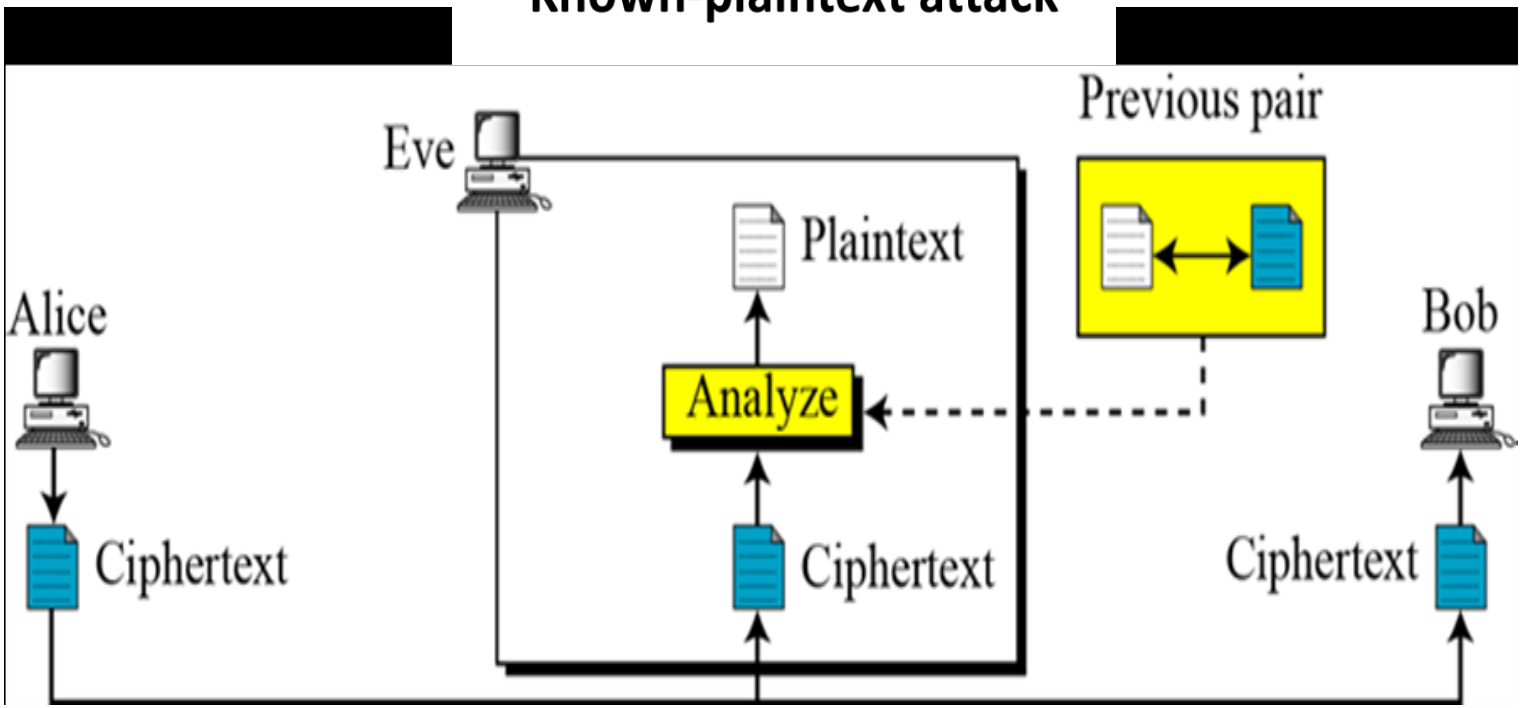
Cryptanalysis and Attacks on Cryptosystems

- 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.

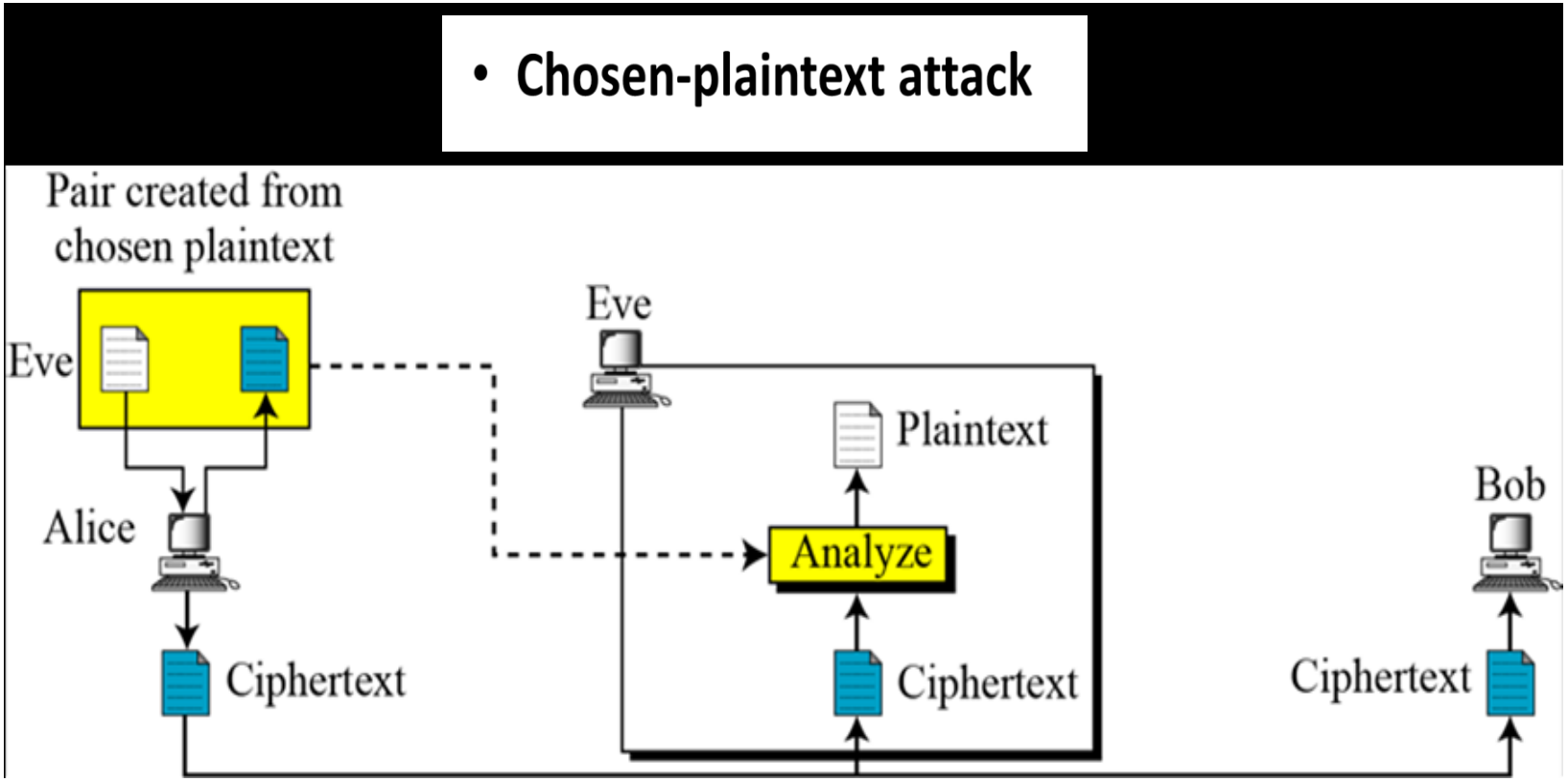


Known-plaintext attack (know/suspect plaintext & – ciphertext to attack cipher): The attacker knows or can guess the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext blocks using this information. This may be done by determining the key used to encrypt the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