Cryptography: An Introduction

Data Encryption & Security (CEN-451)

Spring 2025 (BSE-8A&B)

Basic Terminologies

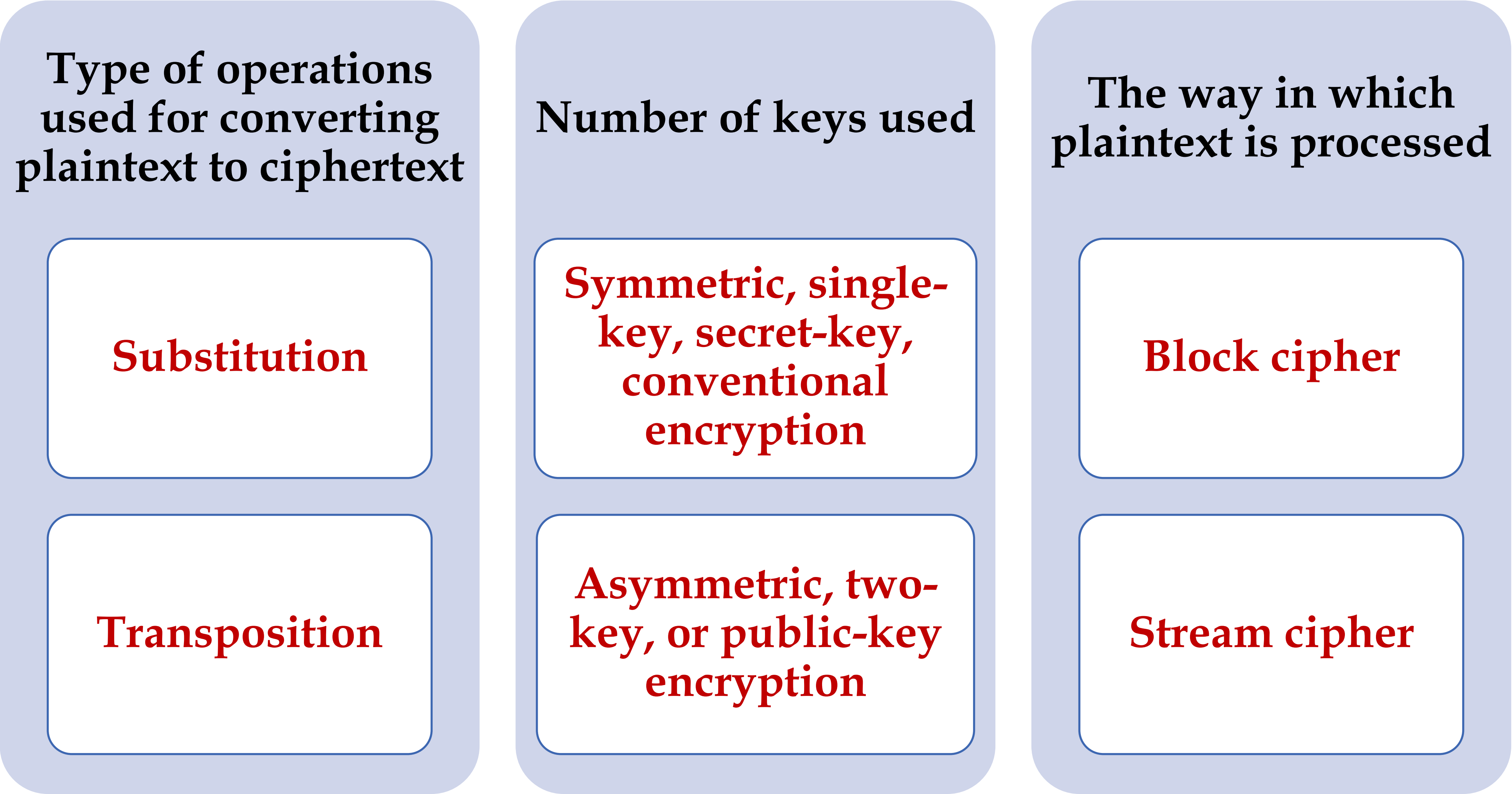
- **Plaintext:** the original intelligible message.
- **Ciphertext:** the coded unintelligible message.
- **Enciphering\Encryption:** the process of converting plaintext to ciphertext.
- **Deciphering\Decryption:** the process of restoring plaintext from ciphertext.

Basic Terminologies (Cont.)

- **Cryptography:** the study of encryption.
- **Cryptanalysis:** techniques used for deciphering a message without any knowledge of the enciphering details.
- **Cryptology:** The field of science that encompasses cryptography and cryptanalysis together.

Cryptographic Systems

- Cryptographic systems are characterized by three dimensions:



Type of operations used for converting plaintext to ciphertext	Number of keys used	The way in which plaintext is processed
Substitution	Symmetric, single-key, secret-key, conventional encryption	Block cipher
Transposition	Asymmetric, two-key, or public-key encryption	Stream cipher

Cryptographic Systems (Cont.)

Type of operations used for transforming plaintext to ciphertext:

- All encryption algorithms are based on two general principles:

  a. **Substitution,** in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element.

  b. **Transposition**, in which elements in the plaintext are rearranged.

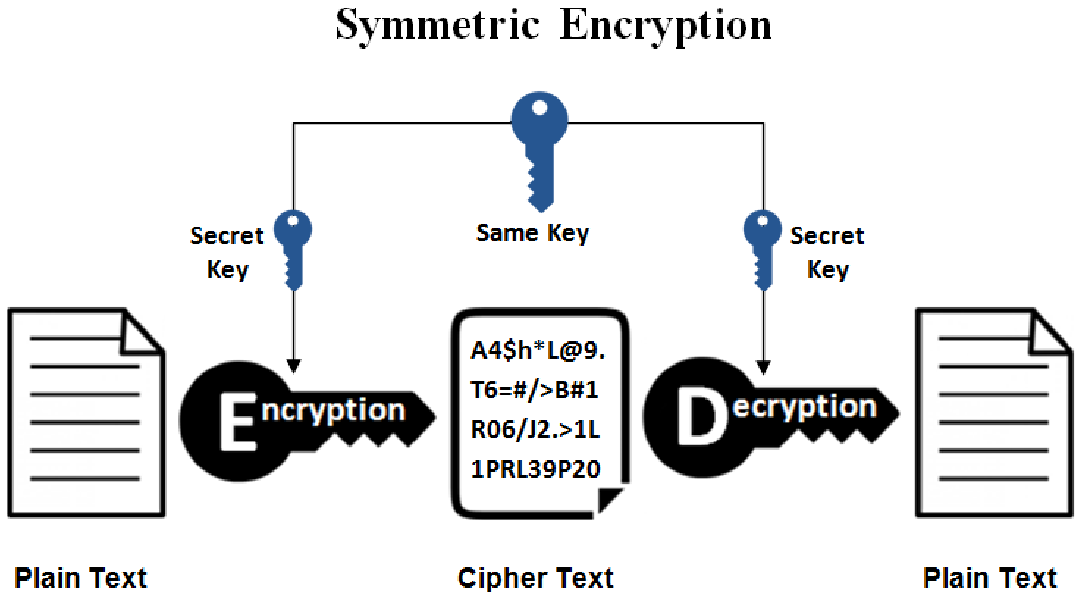
Cryptographic Systems (Cont.)

The way in which the plaintext is processed:

- **Block cipher** processes the input one block of elements at a time, producing an output block for each input block.
- **Stream cipher** processes the input elements continuously, producing output one element at a time, as it goes along.

Cryptographic Algorithms

- Cryptographic algorithms can be grouped into:
  1. **Symmetric-key Algorithms:** cryptography algorithms that use the **same cryptographic keys** for both encryption and decryption.

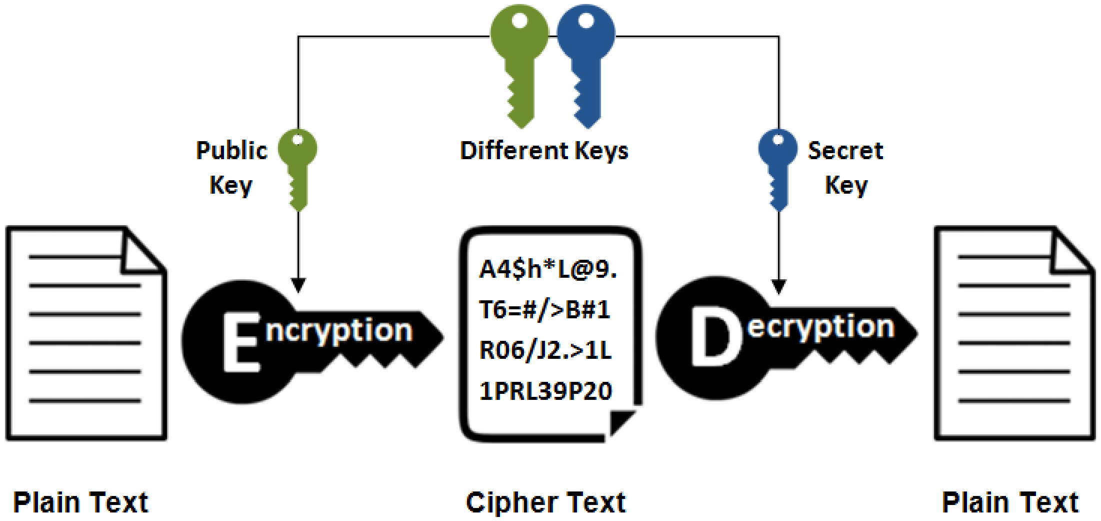


Cryptographic Algorithms (Cont.)

- Cryptographic algorithms can be grouped into:

  2. **Asymmetric-key Algorithms:** cryptography algorithms that uses **pairs of keys**, i.e. public keys and private keys, to encrypt and decrypt data.

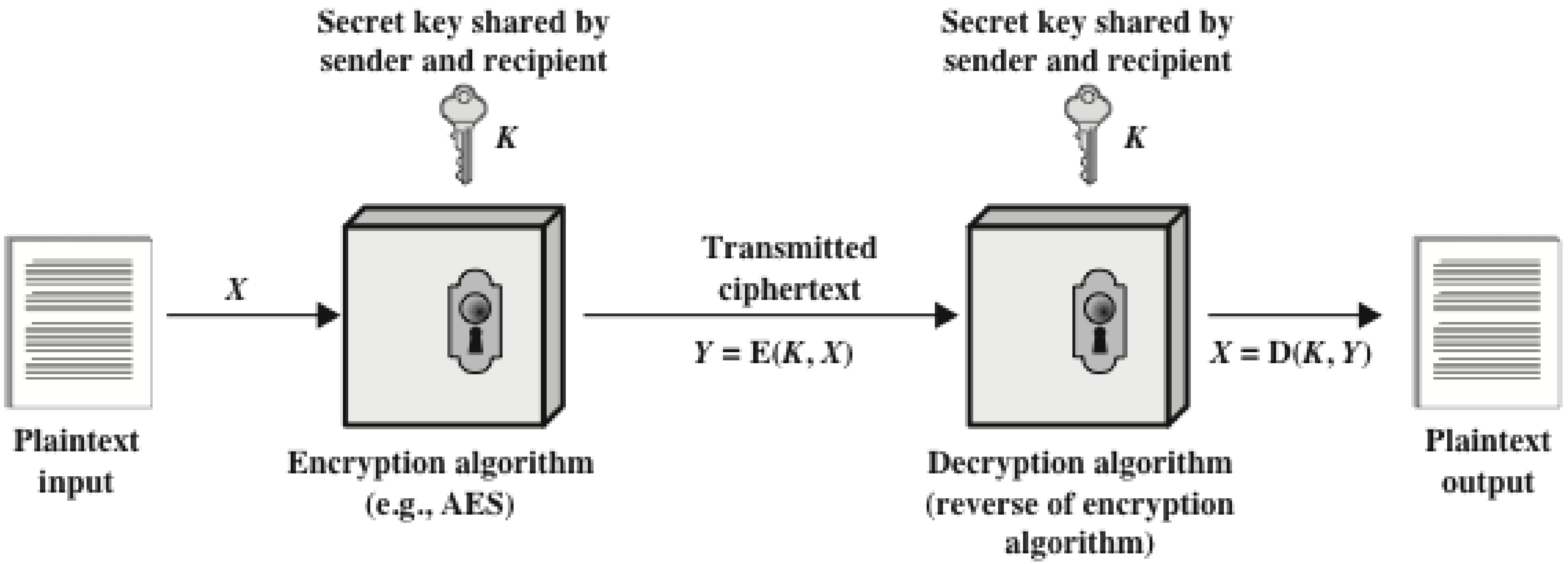
Asymmetric Encryption



Cryptographic Algorithms (Cont.)

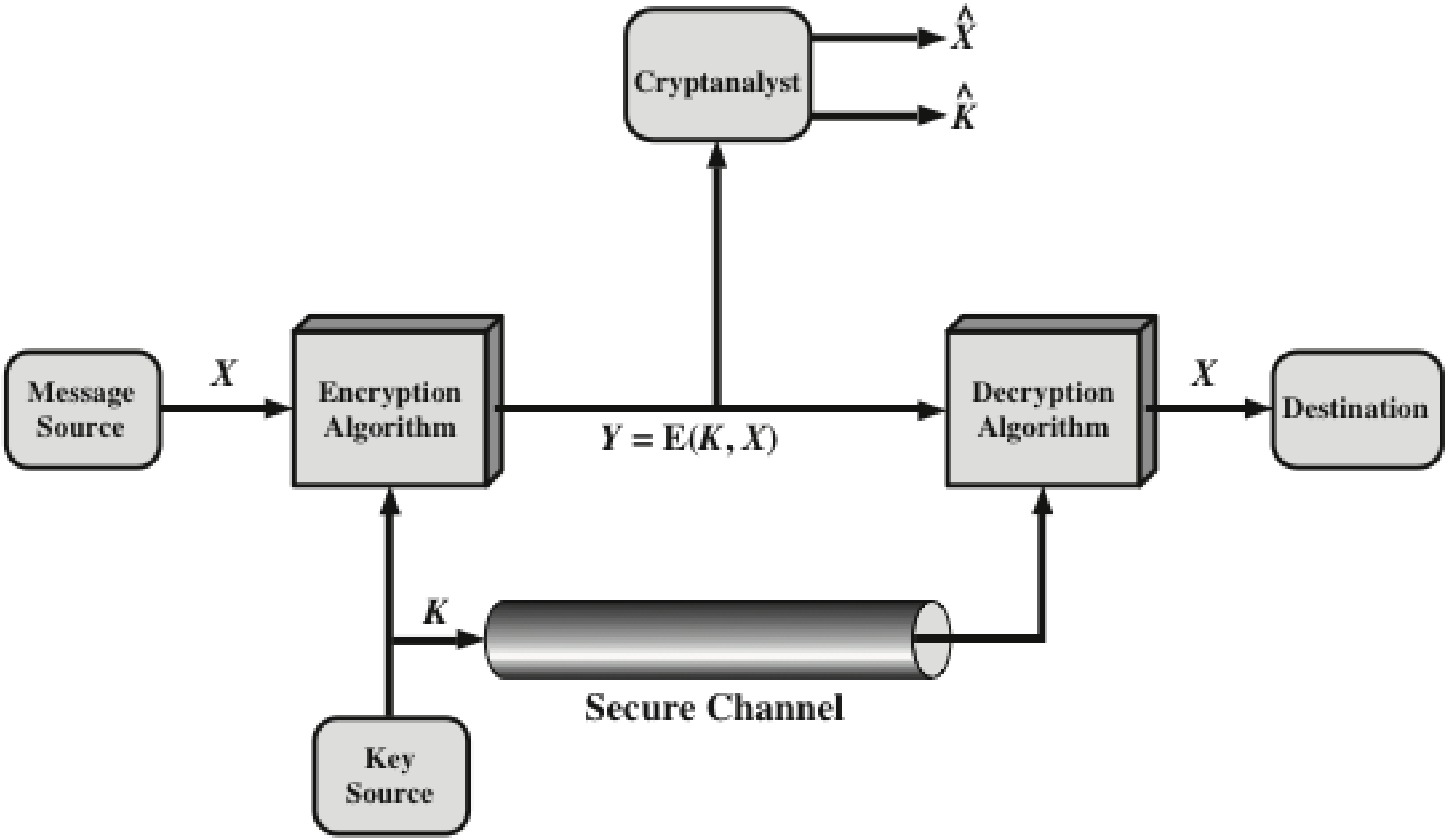
- **Symmetric Encryption** is used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys and passwords.
- **Asymmetric Encryption** is used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures.

Symmetric Encryption


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

A general model for the symmetric encryption.

Symmetric Encryption (Cont.)



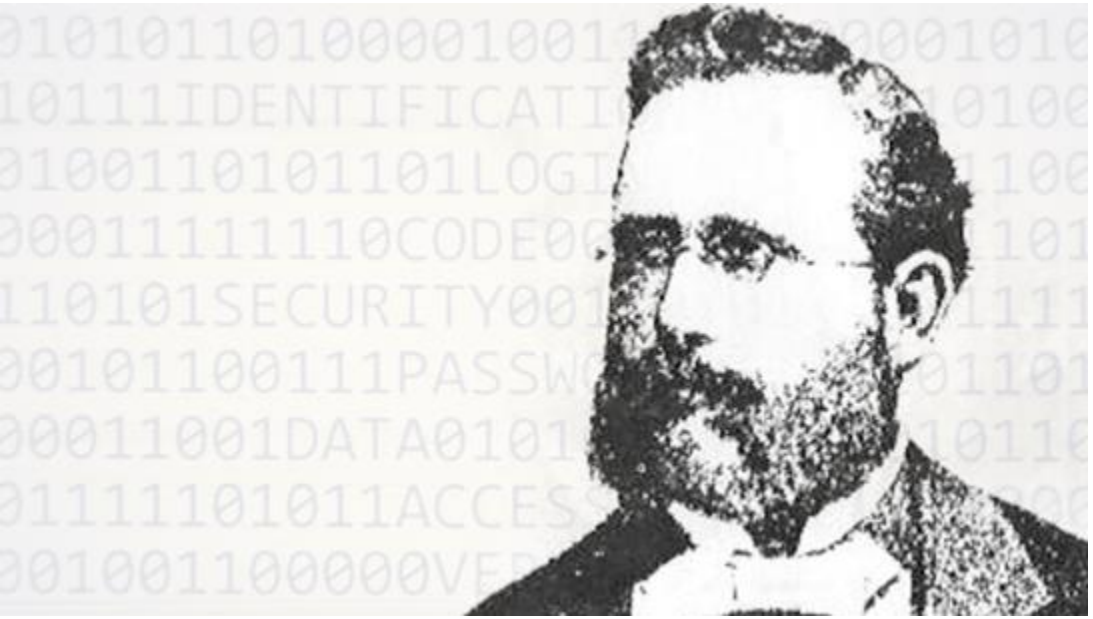
Symmetric Encryption (Cont.)

Properties of secret key in symmetric encryption:

- The **key** is input to **encryption algorithm** along with **plaintext**.
- The **key** is a value independent of the **plaintext** and the **algorithm**.
- The **algorithm** will produce a different output depending on the specific **key** being used. Hence, for a given message, two different **keys** will produce two different **ciphertexts**.
- The **encryption algorithm** performs various substitutions and transpositions on the **plaintext**, where the exact substitutions and transpositions depends on the **key**.

Kerckhoff’s Principle

- **Kerckhoff’s principle:** one should always assume that the adversary knows the **encryption/decryption algorithm**. The resistance of the cipher to attack must be based only on the secrecy of the key.



Kerckhoff's Principle (Cont.)

- It is **impractical** to decrypt a message on the basis of ciphertext plus knowledge of encryption/decryption algorithm.
- There is no need to keep the algorithm secret; but only **keep the key secret**. ***This feature makes symmetric key feasible for widespread use. Hence, manufacturers can and have developed low-cost chip implementations of data encryption algorithms***.
- With the use of symmetric encryption, the principal security problem is maintaining the **secrecy of key**.

Kerckhoff's Principle (Cont.)

- Cipher algorithms may be:
  - Open-source *(the algorithmic process is in the public domain while the key is selected by a user and is private)*.
  - Closed-source *(the process is developed for use in specific domains, such as the military, and the algorithm itself is not in the public domain)*.

Cryptanalysis and Brute-Force

- There are two general approaches for attacking a conventional encryption scheme:
  - **Cryptanalysis,** rely on nature of the algorithm plus some general characteristics of plaintext or plaintext–ciphertext pairs. This attack attempts to deduce a specific plaintext or the key being used.
  - **Brute-force attack**, the attacker tries every possible key on a piece of ciphertext until an intelligible translation is obtained. *On average, half of all possible keys must be tried to achieve success!*

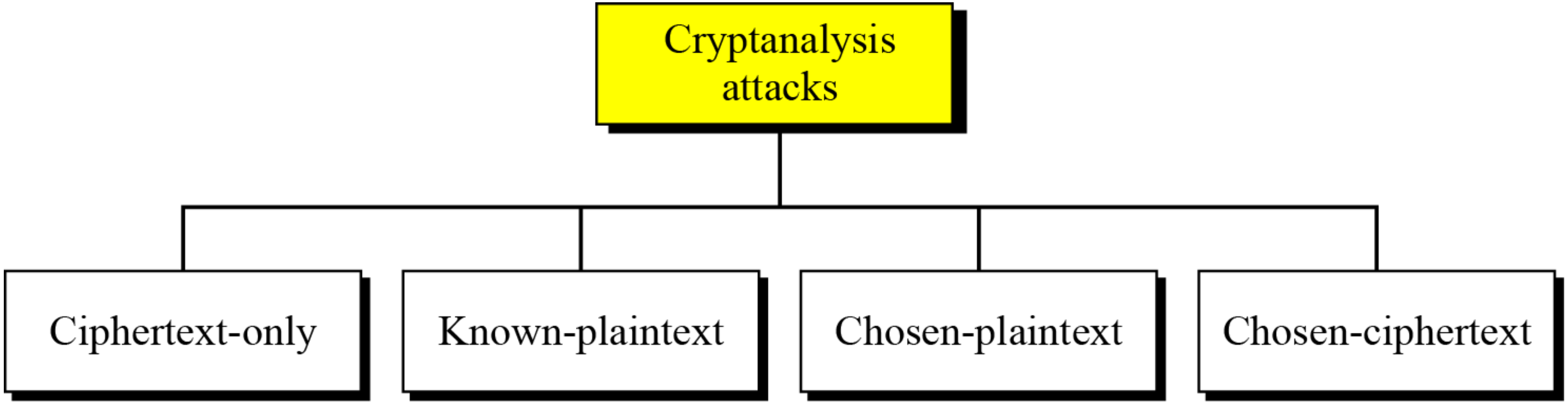
Cryptanalysis and Brute-Force (Cont.)

- In brute-force attack, the attack is proportional to **key size**.

Key Size (bits)	**Number of Alternative Keys**	**Time required at 1 decryption/μs**	**Time required at 10^6 decryptions/μs**
32	$2^{32} = 4.3 \times 10^9$	35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{36} years	5.9×10^{30} years

Cryptanalysis

- As **cryptography** is the science and art of creating secret codes, **cryptanalysis** is the science and art of breaking those codes.
- There are four common types of cryptanalysis attacks based on the amount of information known to the **cryptanalyst**:



Cryptanalysis attacks

Ciphertext-only

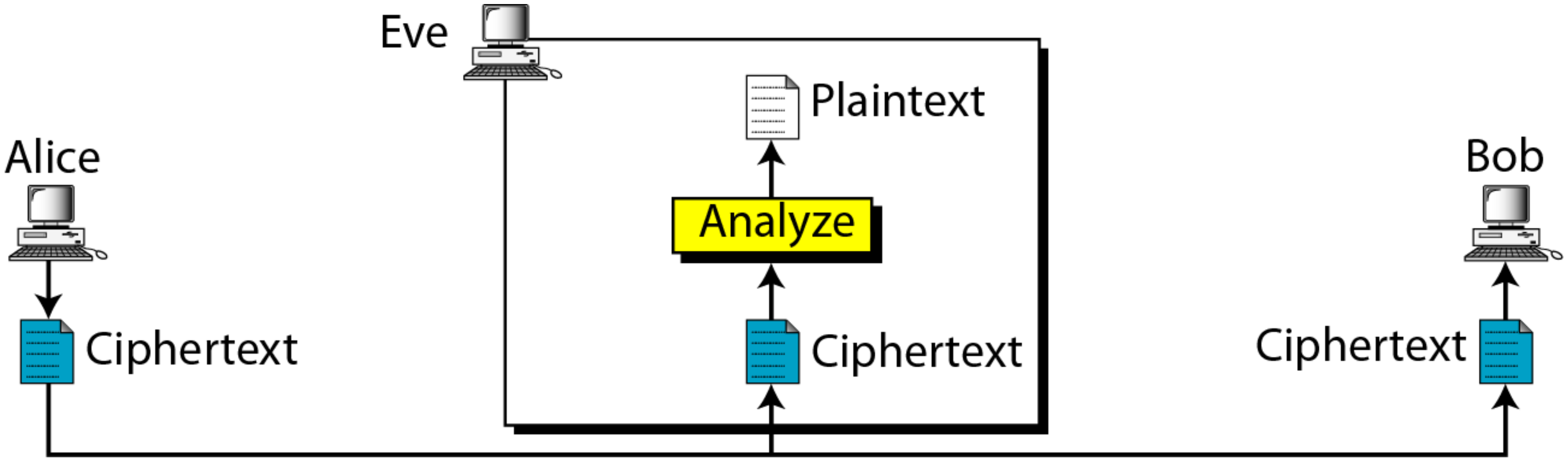
Known-plaintext

Chosen-plaintext

Chosen-ciphertext

Ciphertext-only Attack

- The adversary has access to some **ciphertext** and tries to find the corresponding **key** or **plaintext**.
- This is the most difficult attack for cryptanalyst since ciphertext is all that is available (**note:** in some cases, not even the encryption algorithm is known!).



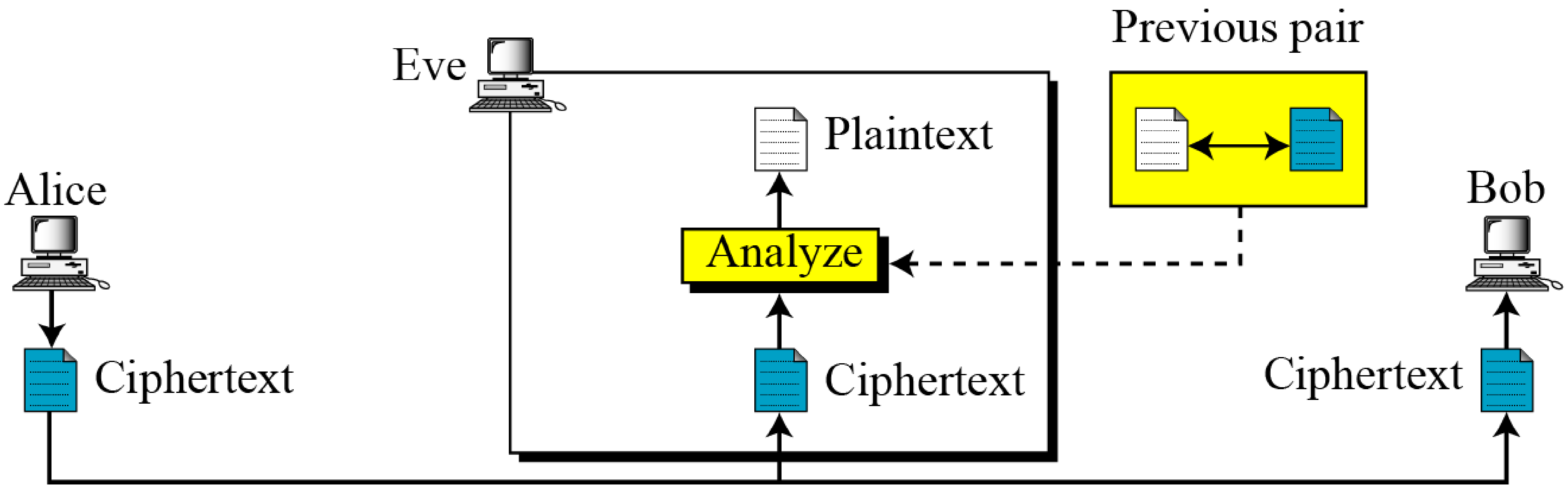
Ciphertext-only Attack (Cont.)

- **Various methods can be used in ciphertext-only attack. The three most common are:**

1. **Brute-Force Attack**, an exhaustive key search method. To prevent this type of attack, the number of possible keys must be very large.
2. **Statistical Attack**, use of inherent characteristic of the language, e.g. English or French.
3. **Pattern Attack**, make use of patterns in ciphertext.

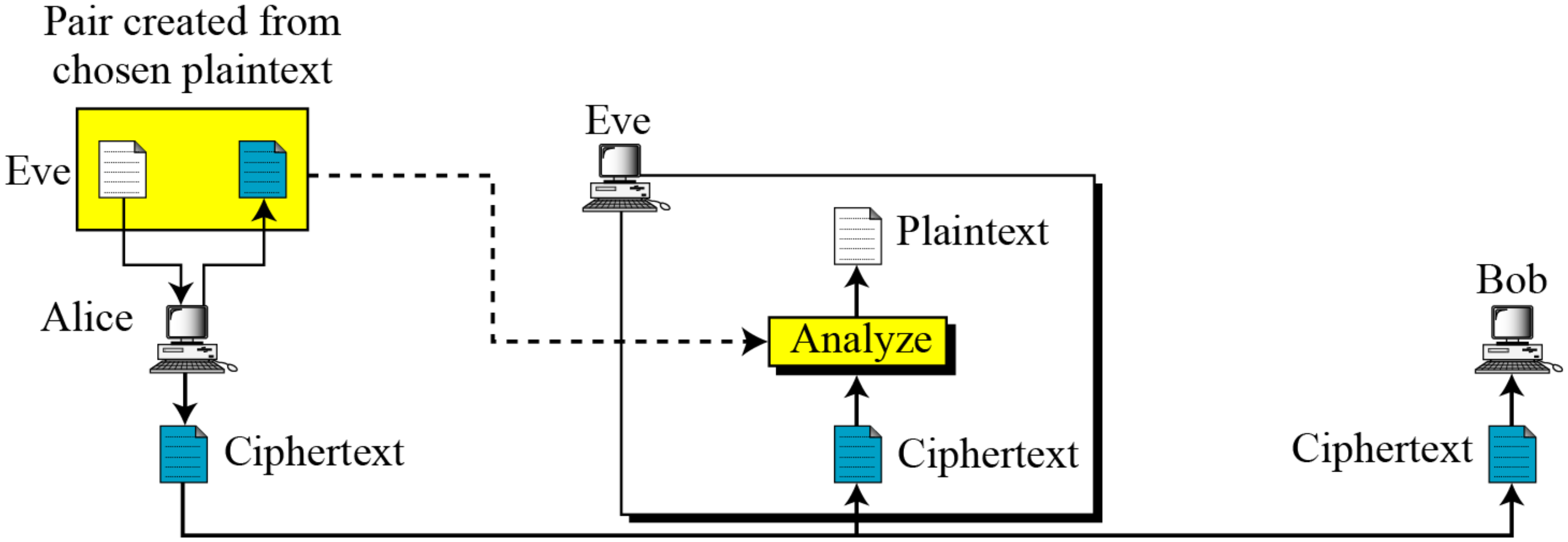
Known-Plaintext Attack

- The attacker has earlier access to **plaintext/ciphertext** pair which is used to attack newly intercepted **ciphertext**.



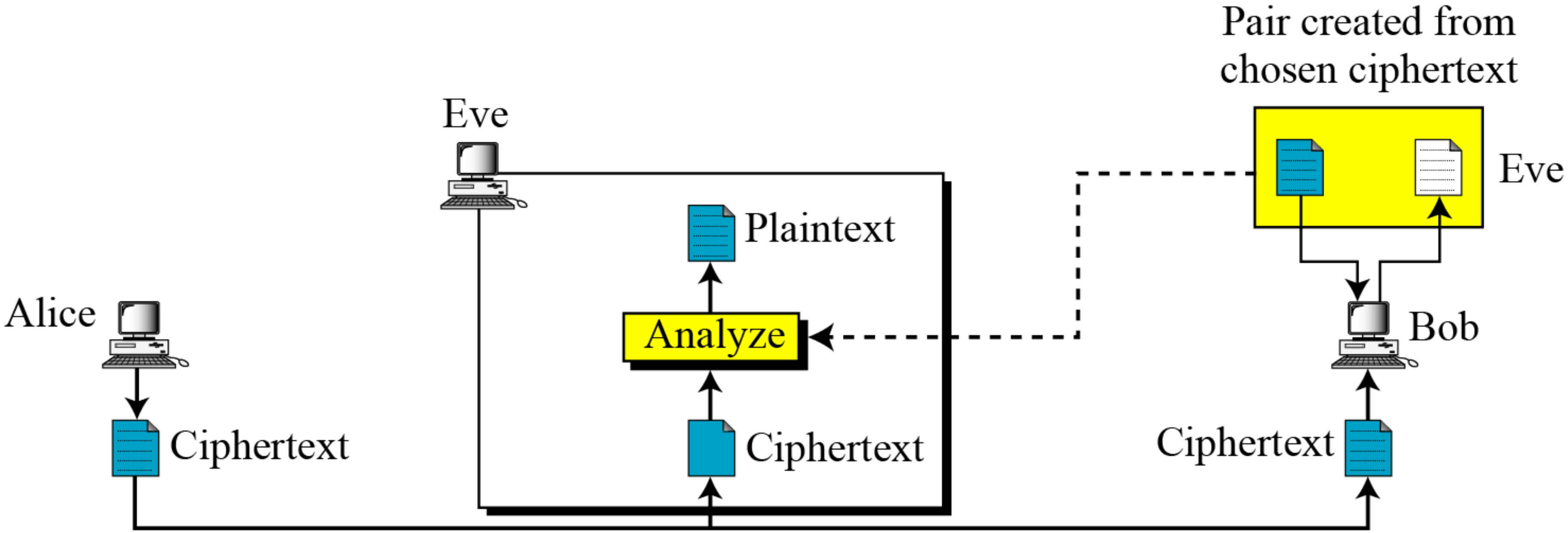
Chosen-Plaintext Attack

- Similar to **known-plaintext** attack but the **plaintext/ciphertext** pair is chosen by attacker.
- **E.g.** analyst is able to get the source to generate messages chosen by the analyst, then use the choose plaintext and the intercept chiphertext pairs for the attack.

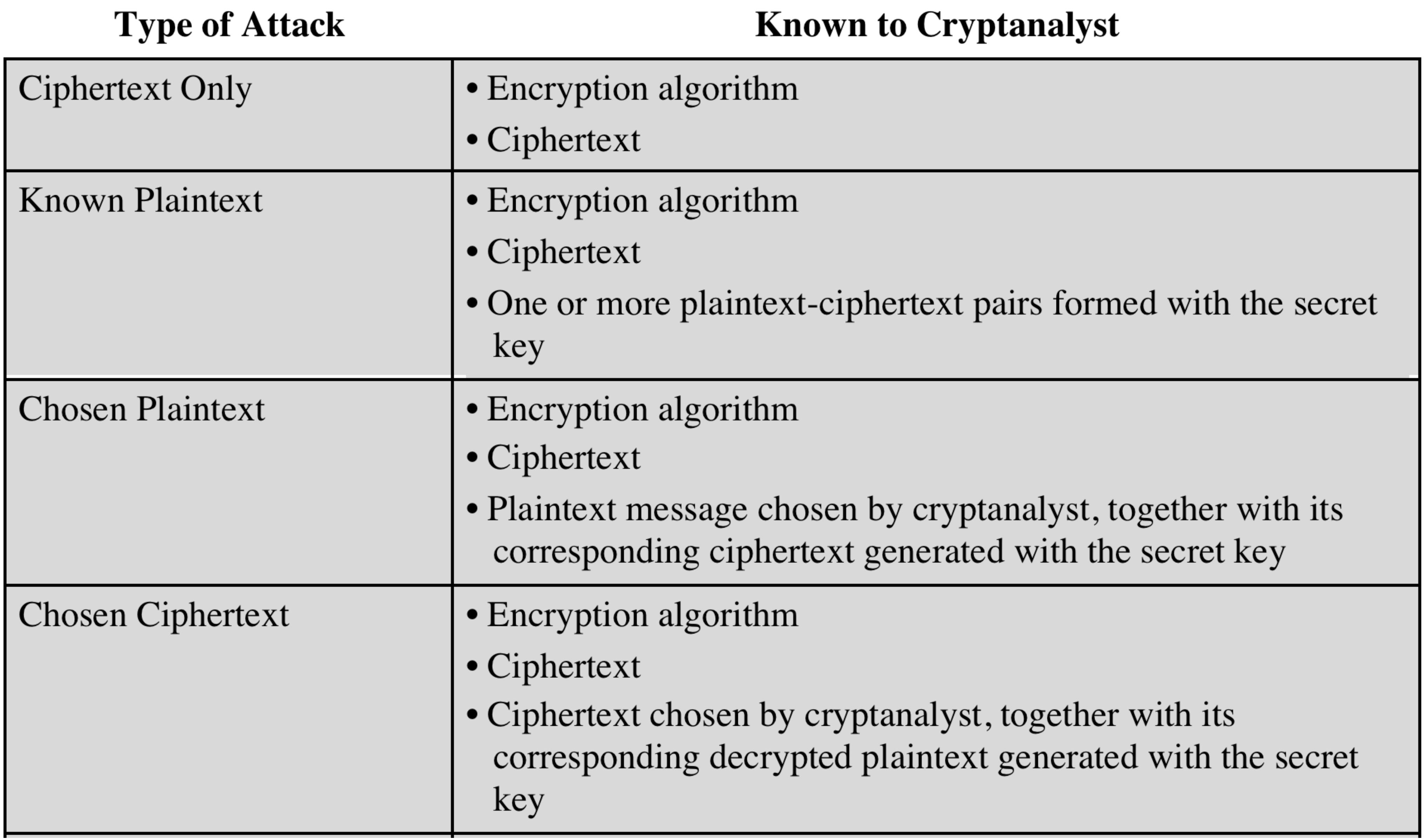


Chosen-Ciphertext Attack

- Similar to **chosen-plaintext** attack but the attacker choses ciphertext and decrypts it to form **ciphertext/plaintext** pair.
- **E.g.** the analyst has access to destination and chooses some ciphertext and decrypts it to form a **plaintext/ciphertext** pair.



Cryptanalysis Attack Summary



Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Cryptanalysis Attack Summary (Cont.)

- Only **relatively weak algorithms** fail to withstand a **ciphertext-only** attack.

- In **Known-Plaintext Attack**, **Chosen-Plaintext Attack** and **Chosen-Ciphertext Attack**, the attacks are easier to implement due to having more information to use for analysis.

Encryption Scheme Security Requirements

Unconditionally secure:

- No matter how much effort an opponent has, it is **impossible** for him/her to decrypt the ciphertext since the required information is not there.

Computationally secure:

- The **cost** of breaking the cipher exceeds the value of the encrypted information.
- The **time** required to break the cipher exceeds the useful lifetime of the information.

Thank You!

Government Access to Keys!

Government Access to Keys (GAK)

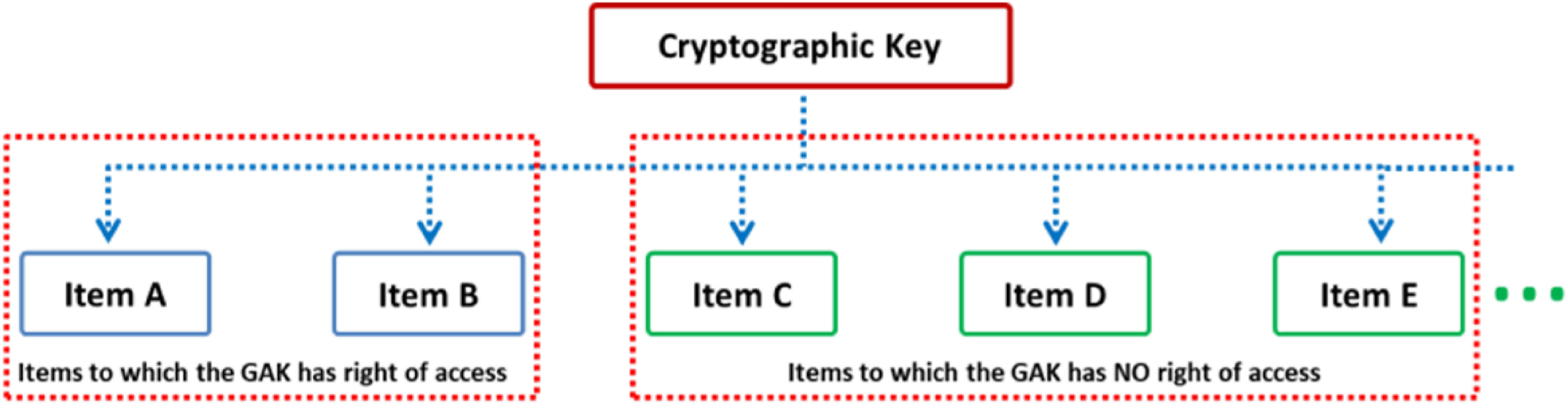
- Government Access to Keys (GAK) refers to the statutory obligation of individuals and organizations to disclose their cryptographic keys to government agencies.
- It means that software companies will give copies of all keys (or at least enough of the key such that the remainder can be cracked) to the government.
- Law enforcement agencies around the world acquire and use these cryptographic keys to monitor suspicious communication and collect evidence of cybercrimes in the interests of national security.

- The government promises that it will hold on to the keys in a secure manner and only use them when a court issues a warrant to do so.
- To the government, this issue is similar to the ability to wiretap phones.

- Government agencies often use **key escrow** for uninterrupted access to keys.
- Key escrow is a key exchange arrangement in which essential cryptographic keys are stored with a third party in escrow.
- The third party can use or allow others to use the encryption keys under certain predefined circumstances.
- The third party, with regard to GAK, is generally a government agency that may use the encryption keys to decipher digital evidence under authorization or a warrant from a court of law.

- There is growing concern about the privacy and security of cryptographic keys and information.
- Government agencies are responsible for protecting these keys.
- Such agencies generally use a single key to protect other keys, which is not a good idea, as revealing a single key could expose the other keys.
- These agencies are not aware of how confidential the information protected by the keys is, which makes it difficult to judge how much protection is required.

- In cases where seized keys also protect other information that these agencies have no right to access, the consequences of key revelation cannot be determined, because government agencies are not aware of the information that the keys protect.
- In such cases, the key owner is liable for the consequences of key revelation.
- Before owners hand over their keys to government agencies, they need to be assured that the government agencies will protect these keys according to a sufficiently strong standard to protect their interests.


Cryptographic Key
Item A
Item B
Item C
Item D
Item E
Items to which the GAK has right of access
Items to which the GAK has NO right of access