# Symmetric Key Cryptography

19CSE311 Computer Security
Jevitha KP
Department of CSE

# Terms

- An original message is known as the **plaintext**, while the coded message is called the **ciphertext.**

- The process of converting from plaintext to ciphertext is known as **enciphering** or **encryption**;

- restoring the plaintext from the ciphertext is **deciphering** or **decryption.**

- The many schemes used for encryption constitute the area of study known as **cryptography.**

- Such a scheme is known as a **cryptographic system** or a **cipher.**

- Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis.**

- Cryptanalysis is what the layperson calls “breaking the code.”

- The areas of cryptography and cryptanalysis together are called **cryptology.**

# Symmetric Key Encryption

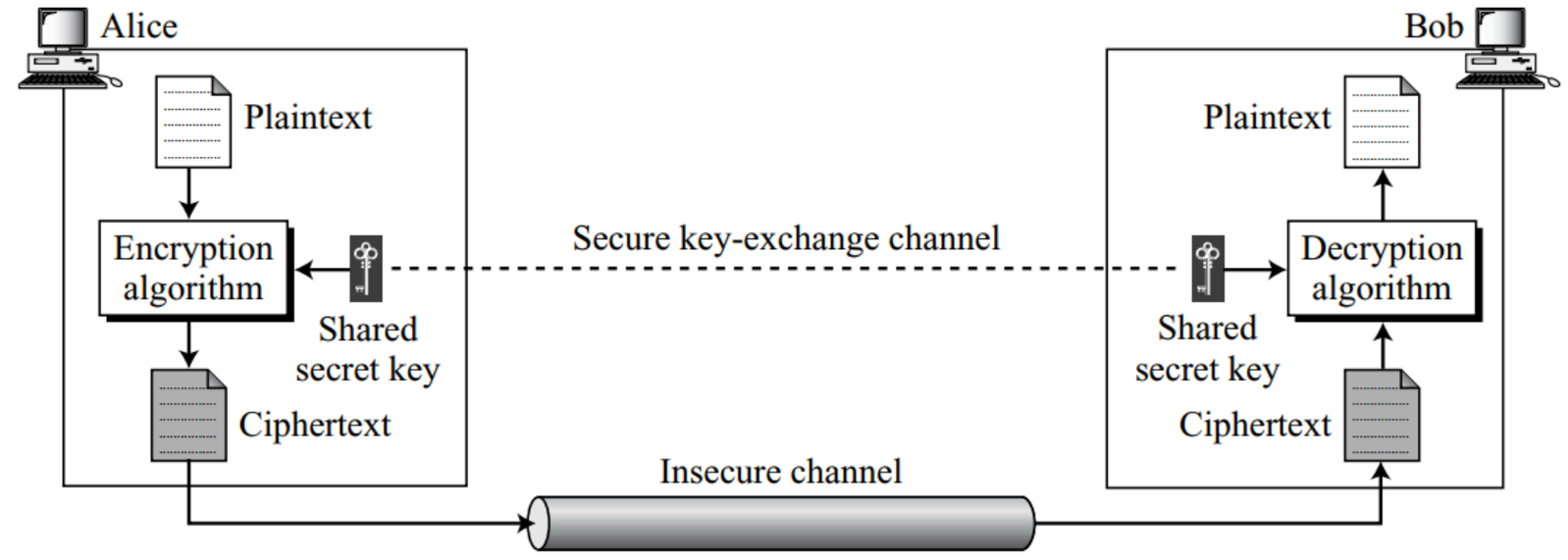
- Symmetric encryption, also referred to as conventional encryption or single-key encryption, was the only type of encryption in use prior to the development of publickey encryption in the 1970s.

- It remains by far the most widely used of the two types of encryption.

- Symmetric-key encipherment uses a **single key** (the key itself may be a set of values) for both encryption and decryption.

- The encryption and decryption algorithms are inverses of each other : they cancel the effect of each other if they are applied one after the other on the same input.

# Symmetric Key Model




Encryption: $C = E_k(P)$ Decryption: $P = D_k(C)$

In which, $D_k(E_k(x)) = E_k(D_k(x)) = x$

**Alice:** $C = E_k(P)$ **Bob:** $P_1 = D_k(C) = D_k(E_k(P)) = P$

# Key exchange

- Alice and Bob need another channel, a secured one, to exchange the secret key.

- Alice and Bob can meet once and exchange the key personally.

- The secured channel here is the face-to-face exchange of the key.

- They can also trust a third party to give them the same key.

- They can create a temporary secret key using another kind of cipher—asymmetric-key ciphers

# No of keys

- Using symmetric-key encipherment, Alice and Bob can use the same key for communication on the other direction, from Bob to Alice.
- This is why the method is called symmetric
- Number of keys - Alice needs another secret key to communicate with another person, say David.
- If there are m people in a group who need to communicate with each other, how many keys are needed?

# No of keys

- The answer is (m × (m – 1))/2 because
  - each person needs m – 1 keys to communicate with the rest of the group,
  - but the key between A and B can be used in both directions.

# Requirements

- We need a **strong encryption algorithm.**
    - The algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.
    - This requirement is usually stated in a stronger form: The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
- Sender and receiver must have obtained copies of the **secret key in a secure fashion** and must keep the key secure.
    - If someone can discover the key and knows the algorithm, all communication using this key is readable.
    - We assume that it is impractical to decrypt a message on the basis of the ciphertext plus knowledge of the encryption/decryption algorithm.
    - We do not need to keep the algorithm secret; we need to keep only the key secret.

# Kerckhoff's Principle

- A cipher may look more secure if we hide both the encryption/decryption algorithm and the secret key, this is not recommended.

- Based on Kerckhoff's principle, one should always assume that the **adversary**, Eve, **knows the encryption/decryption algorithm.**

- The resistance of the cipher to attack must be based only on the secrecy of the key.

- In other words, guessing the key should be so difficult that there is no need to hide the encryption/decryption algorithm.

- This principle manifests itself more clearly when we study modern ciphers.

- There are only a few algorithms for modern ciphers today.

- The **key domain** for each algorithm, however, is so large that it makes it difficult for the adversary to find the key.

# Cryptography

- Cryptographic systems are characterized along three independent dimensions:
    - The **type of operations** used for transforming plaintext to ciphertext.
        - All encryption algorithms are based on two general principles:
            - **substitution**, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and
            - **transposition**, in which elements in the plaintext are rearranged.
            - The fundamental requirement is that no information be lost (i.e., that all operations are reversible).
            - Most systems, referred to as product systems, **involve multiple stages of substitutions and transpositions.**

# Cryptography

- Cryptographic systems are characterized along three independent dimensions:

  - **The number of keys used.**

    - If both sender and receiver use the same key, the system is referred to as **symmetric**, single-key, secret-key, or conventional encryption.

    - If the sender and receiver use different keys, the system is referred to as **asymmetric**, two-key, or public-key encryption.

# Cryptography

- Cryptographic systems are characterized along three independent dimensions:

  - The way in which the **plaintext is processed.**

    - A **block cipher** processes the input one block of elements at a time, producing an output block for each input block.

    - A **stream cipher** processes the input elements continuously, producing output one element at a time, as it goes along

# Cryptanalysis

- As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking those codes.

- We study cryptanalysis techniques not to break other people’s codes, but to learn how vulnerable our cryptosystem is.

- The study of cryptanalysis helps us create better secret codes.

# Cryptanalysis vs brute force

- **Cryptanalysis**:
    - Cryptanalytic attacks rely on the
        - nature of the algorithm
        - some knowledge of the general characteristics of the plaintext or
        - even some sample plaintext–ciphertext pairs.
    - This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
- **Brute-force attack**:
    - The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.
    - On average, half of all possible keys must be tried to achieve success
- If either type of attack succeeds in deducing the key, the effect is catastrophic: **All future and past messages encrypted with that key are compromised.**

# Types of cryptanalytic attacks

- The cryptanalytic attacks are classified based on the amount of information known to the cryptanalyst.

- The most difficult problem is presented when **all that is available is the ciphertext** only.

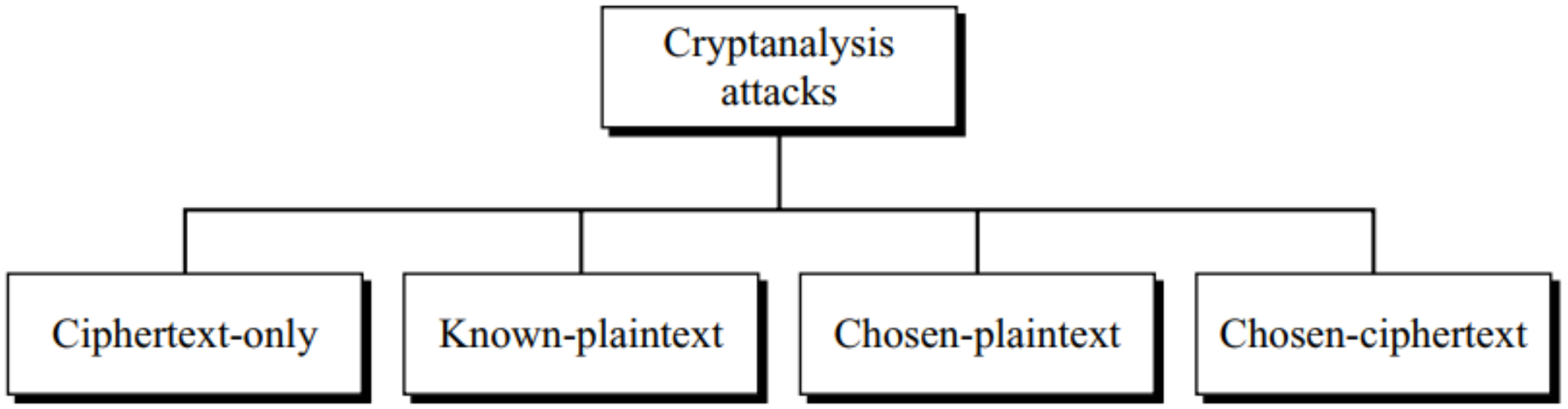
- In some cases, not even the encryption algorithm is known, but in general, we can assume that the opponent does know the algorithm used for encryption.

- One possible attack under these circumstances is the brute-force approach of trying all possible keys.

- If the key space is very large, this becomes impractical.

- Thus, the opponent must rely on an analysis of the ciphertext itself, generally applying **various statistical tests to** it.

# Types of cryptanalytic attacks



# Ciphertext-Only Attack

- In a ciphertext-only attack, Eve has access to only **some ciphertext**.

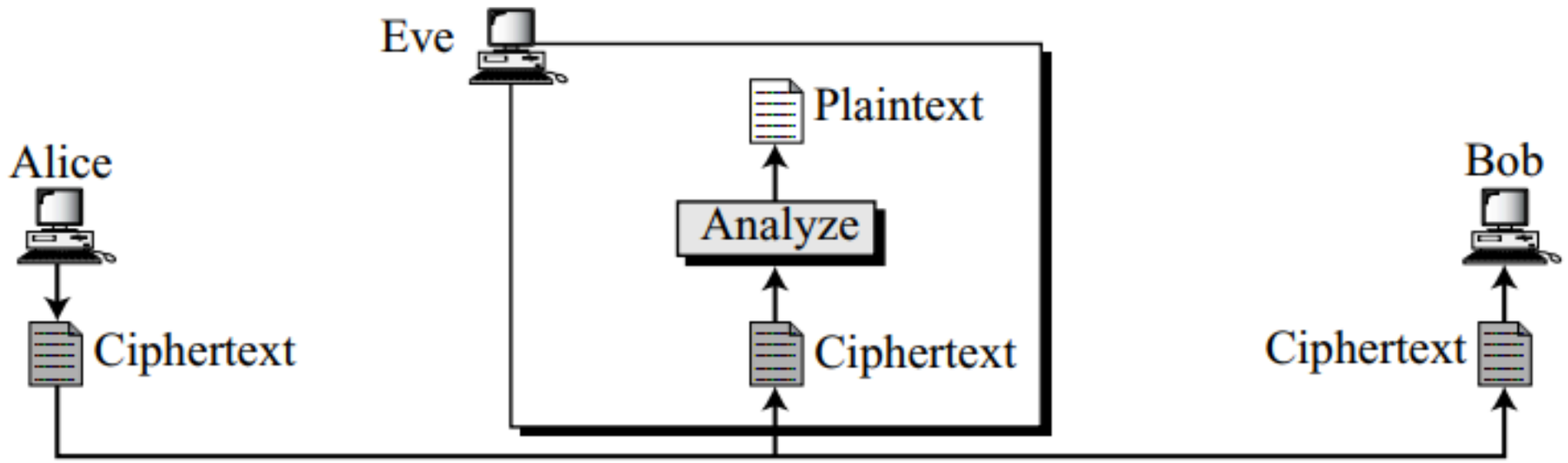
- She tries to find the corresponding key and the plaintext.

- The assumption is that Eve knows the algorithm and can intercept the ciphertext.

- The ciphertext-only attack is the most probable one because Eve **needs only the ciphertext** for this attack.

- To thwart the decryption of a message by an adversary, a cipher must be very resisting to this type of attack.

# Ciphertext-Only Attack



# Ciphertext-Only Attack

- Various methods can be used in ciphertext-only attack:
    - **Brute-Force Attack:**
        - Brute-force method or exhaustive-key-search method tries to use all possible keys.
        - We assume that Eve knows the algorithm and knows the key domain (the list of all possible keys).
        - Using the intercepted cipher, Eve decrypts the ciphertext with every possible key until the plaintext makes sense.
        - Using brute-force attack was a difficult task in the past; it is easier today using a computer.
        - To prevent this type of attack, the number of possible keys must be very large.

# Ciphertext-Only Attack

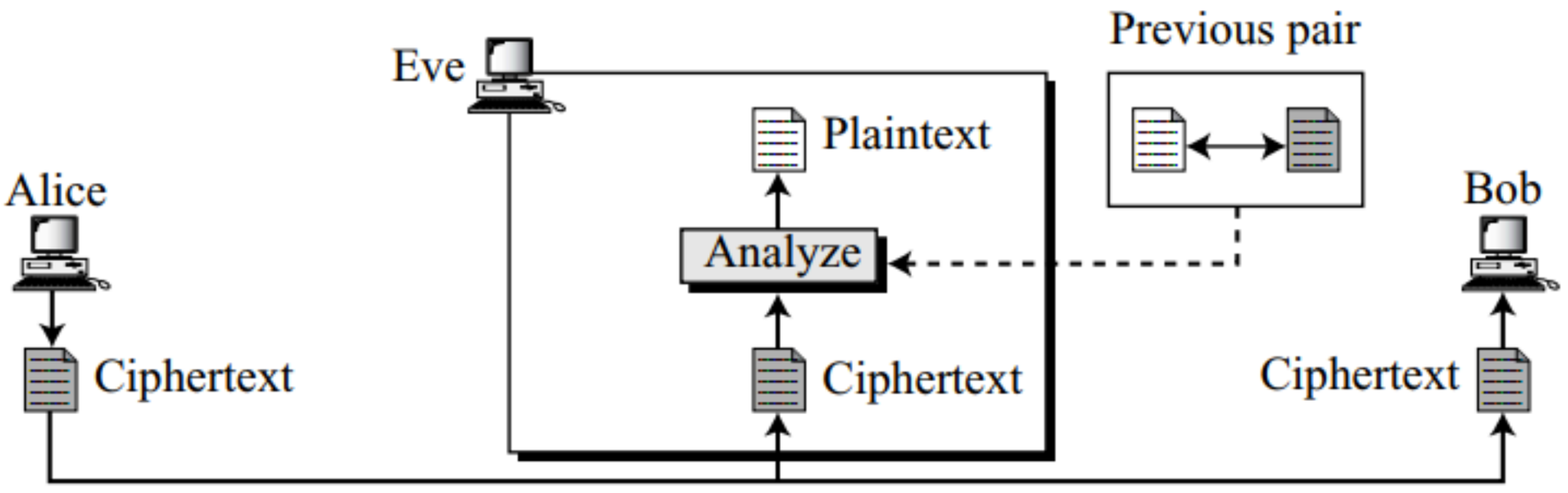
- **Statistical Attack:**
    - The cryptanalyst can benefit from some **inherent characteristics of the plaintext** language to launch a statistical attack.
    - For example, we know that the letter E is the most frequently used letter in English text.
    - The cryptanalyst finds the mostly-used character in the ciphertext and assumes that the corresponding plaintext character is E.
    - After finding a few pairs, the analyst can find the key and use it to decrypt the message.
    - To prevent this type of attack, the **cipher should hide the characteristics of the language.**

# Ciphertext-Only Attack

- **Pattern Attack:**
    - Some ciphers may hide the characteristics of the language, but may **create some patterns** in the ciphertext.
    - A cryptanalyst may use a pattern attack to break the cipher.
    - Therefore, it is important to use ciphers that make the **ciphertext look as random as possible**

# Known-Plaintext Attack

- In a known-plaintext attack, Eve has access to some plaintext/ciphertext pairs in addition to the intercepted ciphertext that she wants to break.

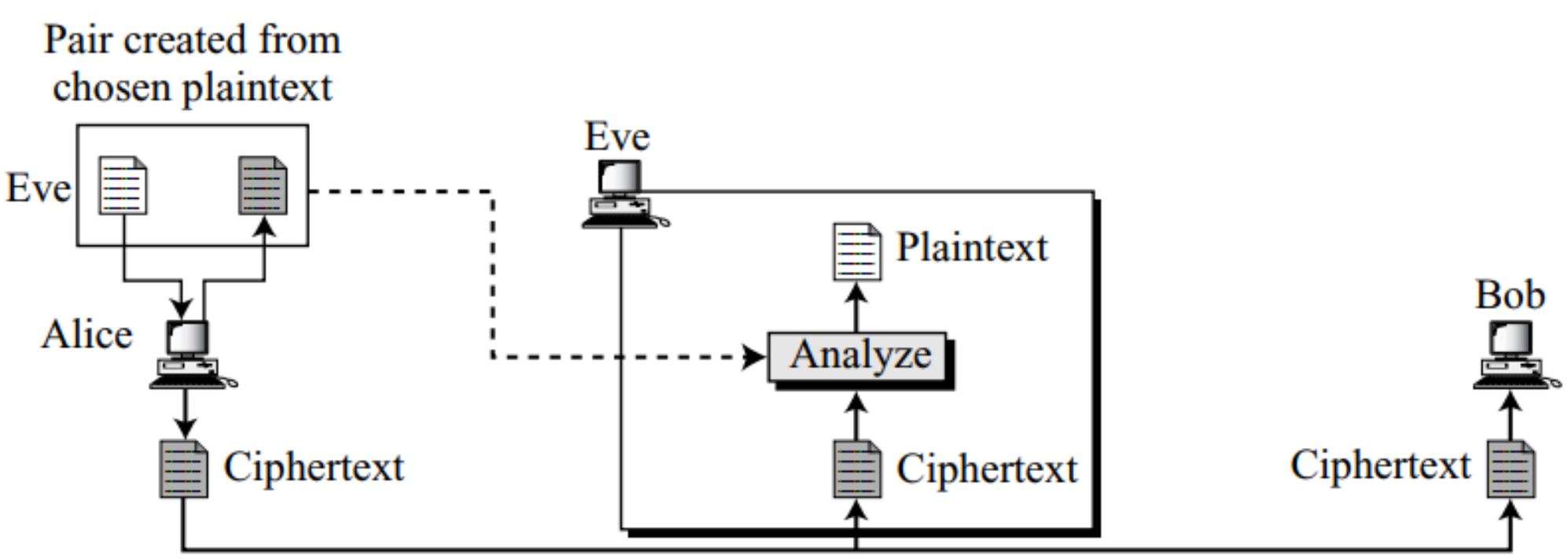


# Known-Plaintext Attack

- The plaintext/ciphertext pairs have been collected earlier.
- For example, Alice has sent a secret message to Bob, but she has later made the contents of the message public.
- Eve has kept both the ciphertext and the plaintext to use them to break the next secret message from Alice to Bob, assuming that Alice has not changed her key.
- Eve uses the relationship between the previous pair to analyze the current ciphertext.
- The same methods used in a **ciphertext-only attack** can be applied here.
- This attack is easier to implement because Eve has more information to use for analysis.
- However, it is less likely to happen because Alice **may have changed her key** or **may have not disclosed the contents of any previous messages**

# Chosen-Plaintext Attack

- The chosen-plaintext attack is similar to the known-plaintext attack, but the plaintext/ ciphertext pairs have been chosen by the attacker herself.



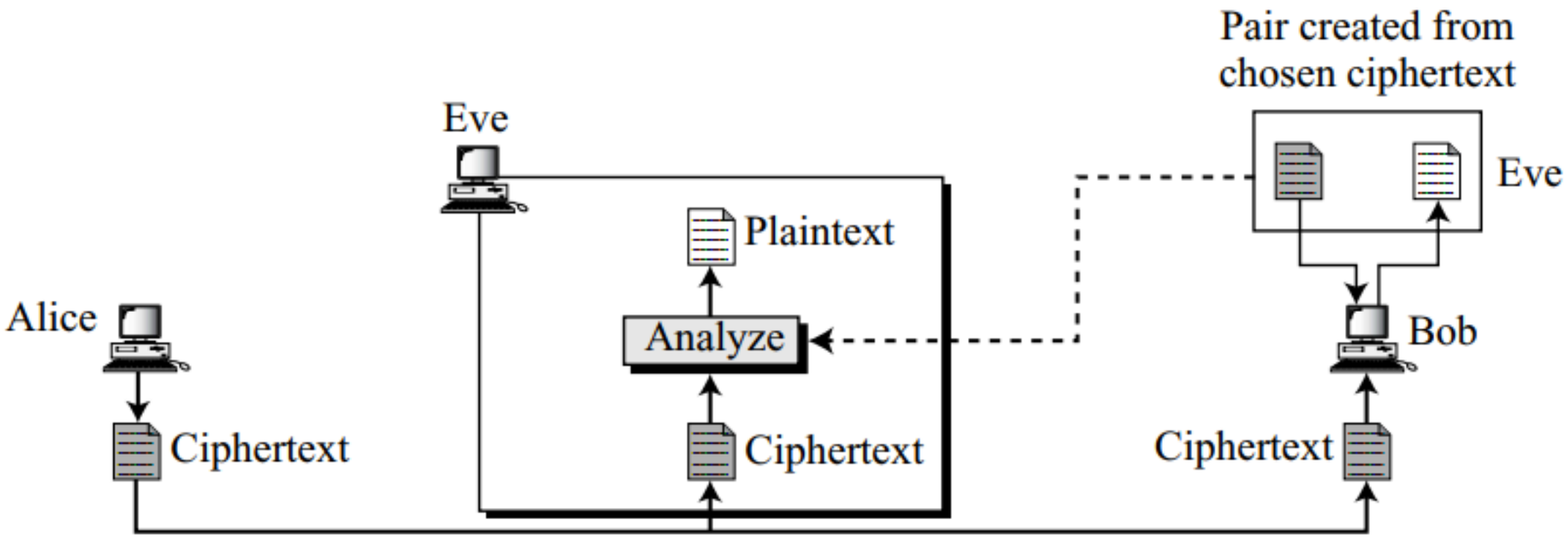
# Chosen-Plaintext Attack

- This can happen, for example, if Eve has access to Alice's computer.
- She can choose some plaintext and intercept the created ciphertext.
- She does not have the key because the key is normally embedded in the software used by the sender.
- This type of attack is much easier to implement, but it is much less likely to happen.

# Chosen-Ciphertext Attack

- The chosen-ciphertext attack is similar to the chosen-plaintext attack, except that Eve chooses some ciphertext and decrypts it to form a ciphertext/plaintext pair.

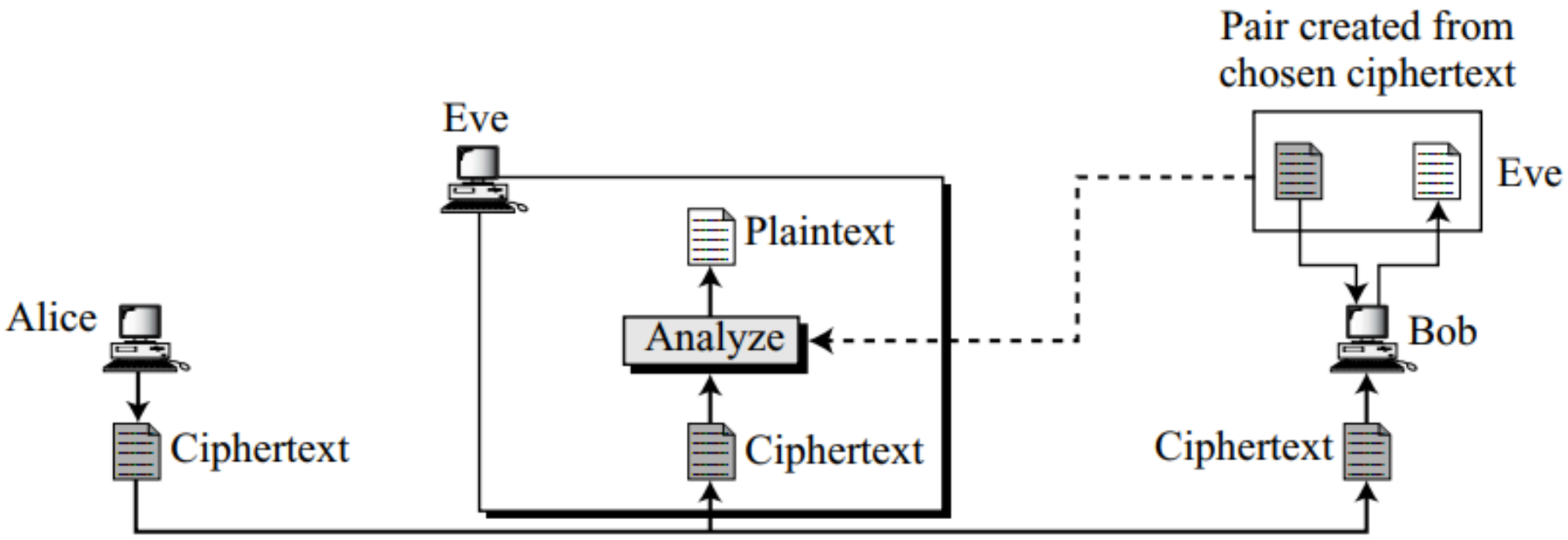
- This can happen if Eve has access to Bob's computer.



# Chosen-Ciphertext Attack

- The chosen-ciphertext attack is similar to the chosen-plaintext attack, except that Eve chooses some ciphertext and decrypts it to form a ciphertext/plaintext pair.

- This can happen if Eve has access to Bob's computer.



# Types of cryptanalytic attacks

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

# Types of cryptanalytic attacks

- To use these approachs, the opponent must have some general idea of the type of plaintext that is concealed, such as English or French text, an EXE file, a Java source listing, an accounting file, and so on

- The ciphertext-only attack is the easiest to defend against because the opponent has the least amount of information to work with.

- In many cases, however, the analyst has more information.

- The analyst may be able to capture one or more plaintext messages as well as their encryptions.

- Or the analyst may know that certain plaintext patterns will appear in a message.

- For example, a file that is encoded in the Postscript format always begins with the same pattern, or there may be a standardized header or banner to an electronic funds transfer message, and so on.

- All these are examples of known plaintext.

- With this knowledge, the analyst may be able to deduce the key on the basis of the way in which the known plaintext is transformed

# Unconditionally secure Algorithm

- An encryption scheme is **unconditionally secure** if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.

- That is, no matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there.

- With the exception of a scheme known as the **one-time pad,** there is no encryption algorithm that is unconditionally secure.

- Therefore, all that the users of an encryption algorithm can strive for is an algorithm that meets one or both of the following criteria:

    - 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.**

# Computationally Secure

- An encryption scheme is said to be **computationally secure** if either of the foregoing two criteria are met.

- Unfortunately, it is very difficult to estimate the amount of effort required to cryptanalyze ciphertext successfully.

- All forms of cryptanalysis for symmetric encryption schemes are designed to exploit the fact that **traces of structure or pattern** in the plaintext may survive encryption and be discernible in the ciphertext.

# Brute Force attack

- A brute-force attack i**nvolves trying every possible key** until an intelligible translation of the ciphertext into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success.
- That is, if there are X different keys, on average an attacker would discover the actual key after **X/2 tries**.
- There is more to a brute-force attack than simply running through all possible keys.
- Unless known plaintext is provided, the analyst must be able to recognize plaintext as plaintext.
- If the message is just plain text in English, then the result pops out easily, although the task of recognizing English would have to be automated.
- If the **text message has been compressed** before encryption, then recognition is more difficult.
- And if the message is some more general type of data, such as a numerical file, and this has been compressed, the problem becomes even more difficult to automate.
- Thus, to supplement the brute-force approach, **some degree of knowledge about the expected plaintext** is needed, and some means of automatically distinguishing plaintext from garble is also needed.

# Decipher

- RJjy rj fkyjw ymj hqfxx
- Qefp fp zbxpxo zfmebo
- Shofjqdqboiyi yi ydjuhuijydw

# Decipher

- RJjy rj fkyjw ymj hqfxx - Meet me after the class = +5
- Qefp fp zbxpxo zfmebo - This is ceasar cipher =  +23
- Shofjqdqboiyi yi ydjuhuijydw - Cryptanalysis is interesting = +16