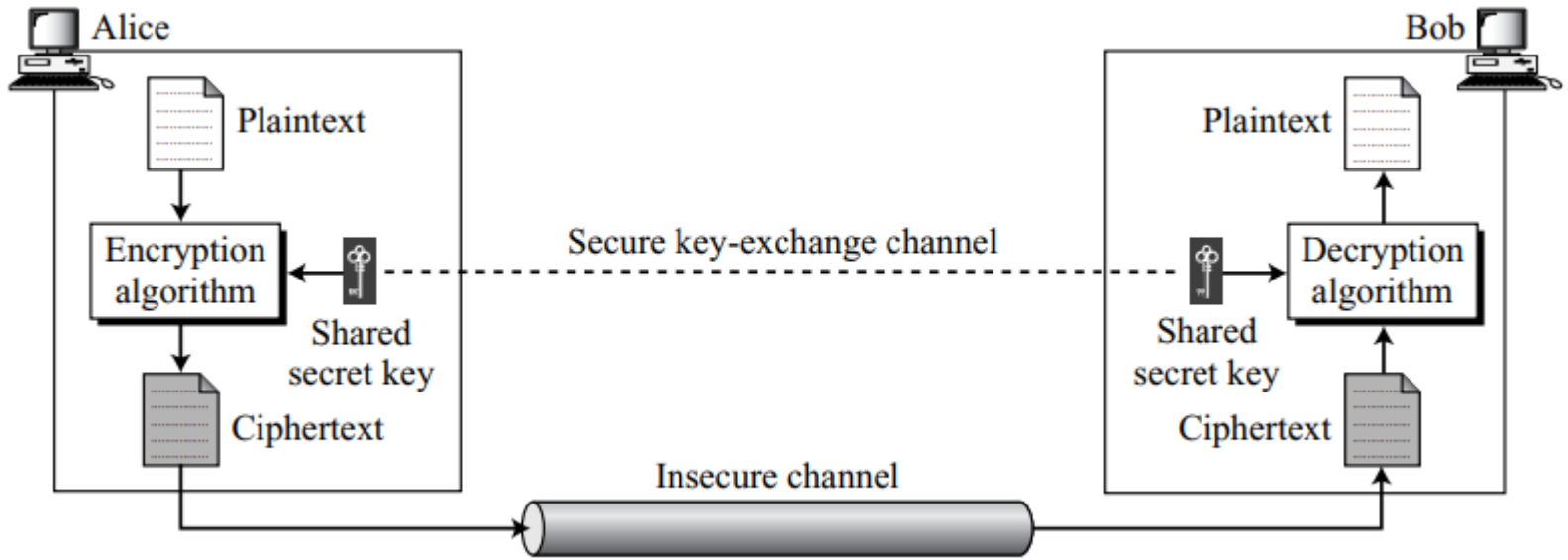
Cryptography and Network Security

Traditional Symmetric-Key Cipher

Introduction

- The original message from Alice to Bob is called plaintext; the message that is sent through the channel is called the ciphertext.
- Alice uses an encryption algorithm and a shared secret key.
- Bob uses a decryption algorithm and the same secret key.
- We refer to encryption and decryption algorithms as ciphers. A key is a set of values (numbers) that the cipher, as an algorithm, operates on.



Introduction

- If P is the plaintext, C is the ciphertext, and K is the key, the encryption algorithm $E_k(x)$ creates the ciphertext from the plaintext.
- The decryption algorithm $D_k(x)$ creates the plaintext from the ciphertext.
- We assume that $E_k(x)$ and $D_k(x)$ are inverses of each other: they cancel the effect of each other if they are applied one after the other on the same input.

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

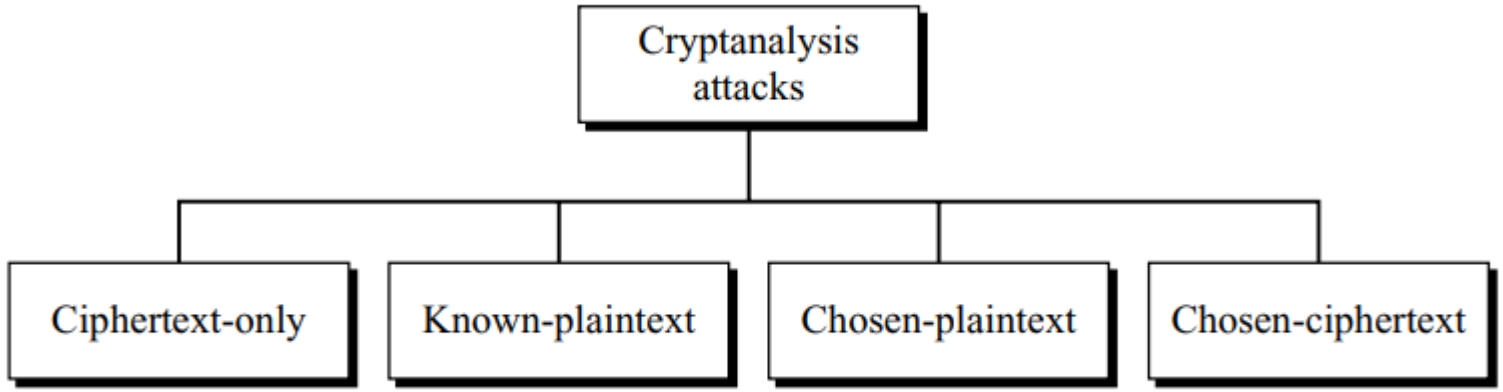
In which, $D_k(E_k(x)) = E_k(D_k(x)) = x$

Kerckhoff's Principle

- 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.
- This principle manifests itself more clearly when we study modern ciphers.
- The **key domain** for each algorithm, however, is so large that it makes it difficult for the adversary to find the key.

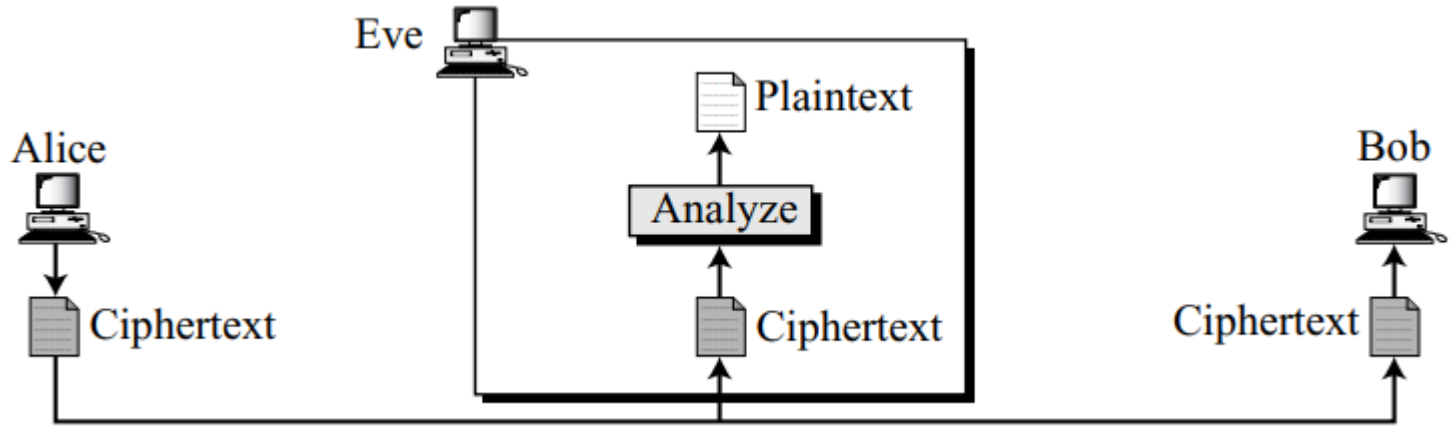
Cryptanalysis

- **Cryptanalysis** is the science and art of breaking those codes.
- In addition to studying cryptography techniques we also need to study cryptanalysis techniques.
- This is needed, 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. There are four common types of cryptanalysis attacks



Cryptanalysis

- **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.

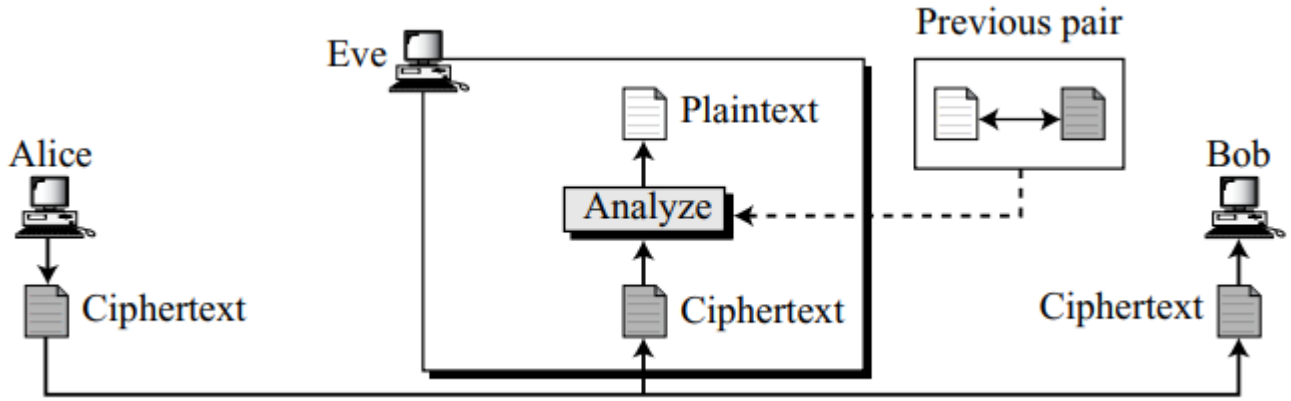


Cryptanalysis

- Various methods can be used in ciphertext-only attack.
  - **Brute-Force Attack** – Eve tries to use all possible keys.
  - **Statistical Attack** – The cryptanalyst can benefit from some inherent characteristics of the plaintext language.
  - **Pattern Attack** – Some ciphers may hide the characteristics of the language, but may create some patterns in the ciphertext. So the ciphertext should look as random as possible.

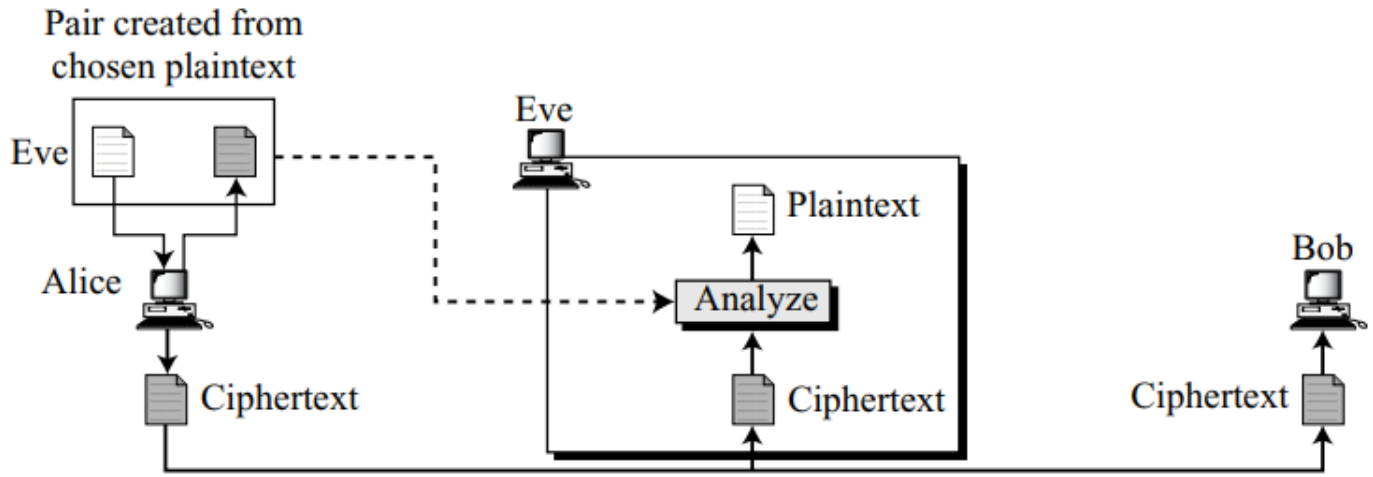
Cryptanalysis

- **Known-Plaintext Attack** –
  - 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.
  - This attack is easier to implement because Eve has more information to use for analysis.



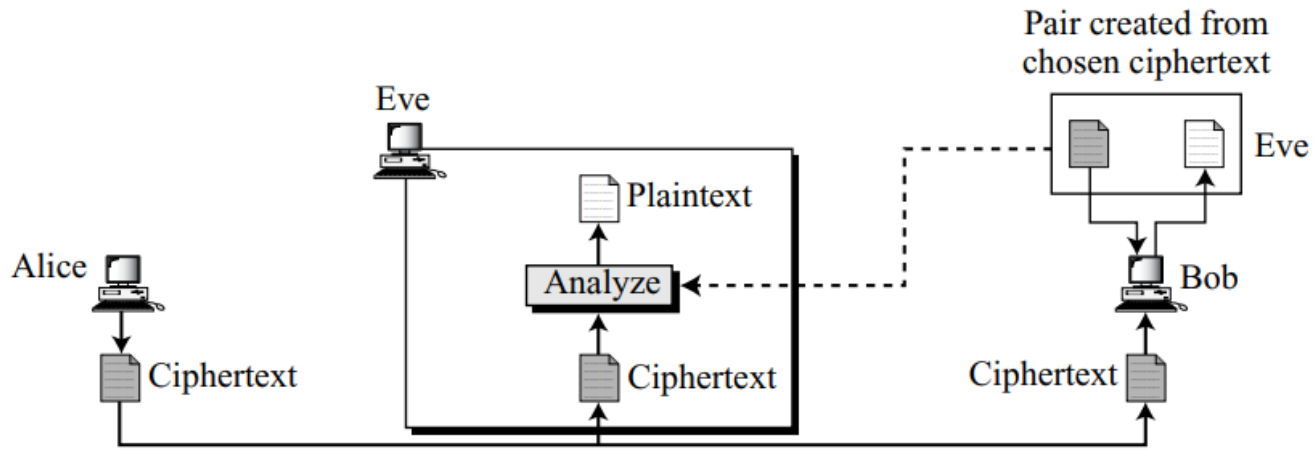
Cryptanalysis

- **Chosen-Plaintext Attack –**
  - If Eve has access to Alice's computer. She can choose some plaintext and intercept the created ciphertext.
  - Of course, 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.



Cryptanalysis

- **Chosen-Ciphertext Attack** –
  - It 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.



Substitution Ciphers

- It replaces one symbol with another.
- **Monoalphabetic Ciphers –**
  - a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text.

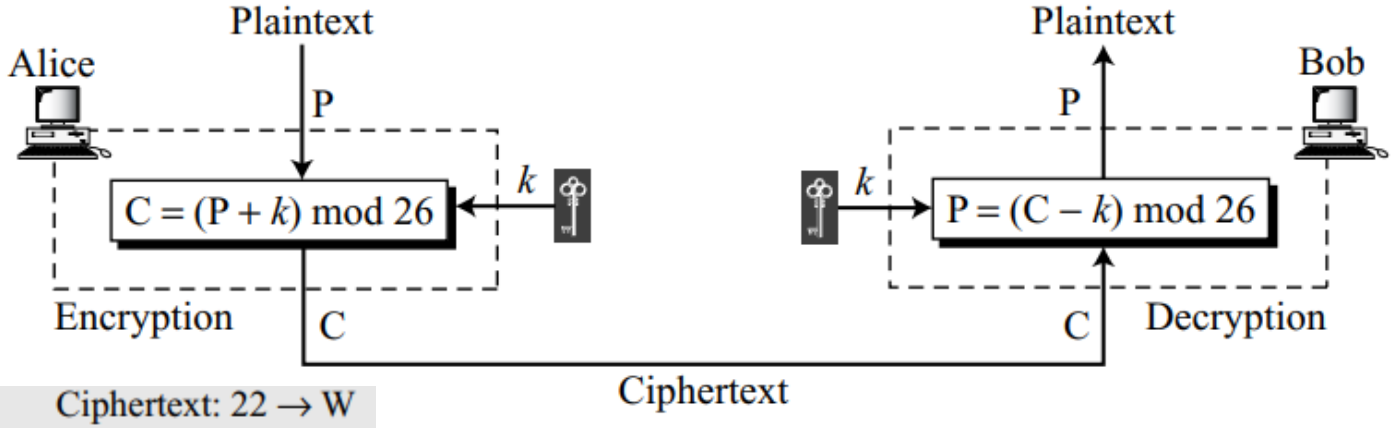
Plaintext: hello **Ciphertext:** KHOOR

  - Following is not a monoalphabetic cipher.

Plaintext: hello **Ciphertext:** ABNZF

Monoalphabetic Ciphers

- **Additive Cipher –**
  - The secret key between Alice and Bob is an integer in Z_{26}.
  - The encryption algorithm adds the key to the plaintext character; the decryption algorithm subtracts the key from the ciphertext character.
  - All operations are done in Z_{26}.



Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Monoalphabetic Ciphers

- **Cryptanalysis for Additive Cipher –**
  - Eve has intercepted the ciphertext “UVACLYFZLJBYL”. Show how she can use a brute-force attack to break the cipher.

K = 1	→	**Plaintext:** tuzbkxeykiaxk
K = 2	→	**Plaintext:** styajwdxjhzwj
K = 3	→	**Plaintext:** rsxzivcwigyvi
K = 4	→	**Plaintext:** qrwyhubvhfxuh
K = 5	→	**Plaintext:** pqvxgtaugewtg
K = 6	→	**Plaintext:** opuwfsztfdvsf
K = 7	→	**Plaintext:** notverysecure

Monoalphabetic Ciphers

- **Cryptanalysis for Additive Cipher** –
  - Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

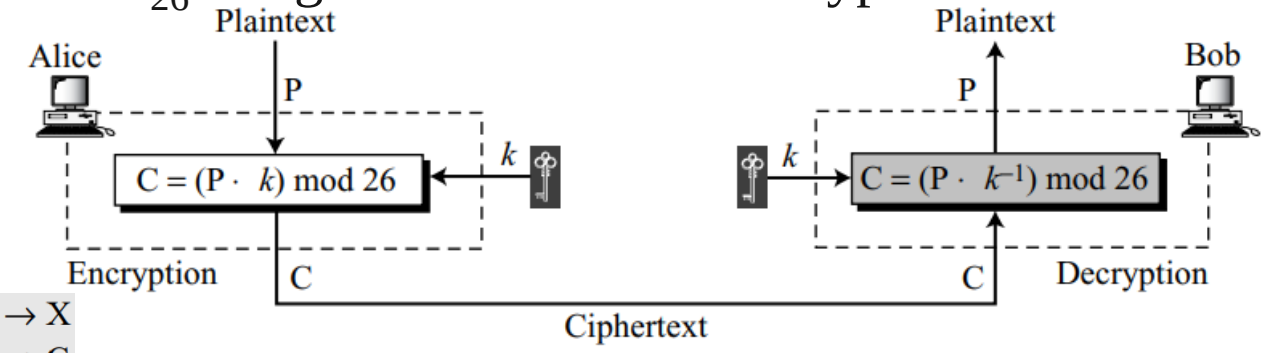
XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

  - When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on. The most common character is I with 14 occurrences. This shows that character I in the ciphertext probably corresponds to the character e in plaintext. This means key = 4. Eve deciphers the text to get

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

Monoalphabetic Ciphers

- **Multiplicative Cipher –**
  - the encryption algorithm specifies multiplication of the plaintext by the key and the decryption algorithm specifies division of the ciphertext by the key.
  - However, since operations are in Z_{26}, decryption here means multiplying by the multiplicative inverse of the key.
  - Note that the key needs to belong to the set Z_{26}^* to guarantee that the encryption and decryption are inverses of each other.



Plaintext: h → 07	Encryption: (07 × 07) mod 26	ciphertext: 23 → X
Plaintext: e → 04	Encryption: (04 × 07) mod 26	ciphertext: 02 → C
Plaintext: l → 11	Encryption: (11 × 07) mod 26	ciphertext: 25 → Z
Plaintext: l → 11	Encryption: (11 × 07) mod 26	ciphertext: 25 → Z
Plaintext: o → 14	Encryption: (14 × 07) mod 26	ciphertext: 20 → U