Network Security

Introduction

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers.

- **Network Security** - measures to protect data during their transmission.

- **Internet Security** - measures to protect data during their transmission over a collection of interconnected network

Network Security

Network security problems can be divided roughly into four closely intertwined areas:

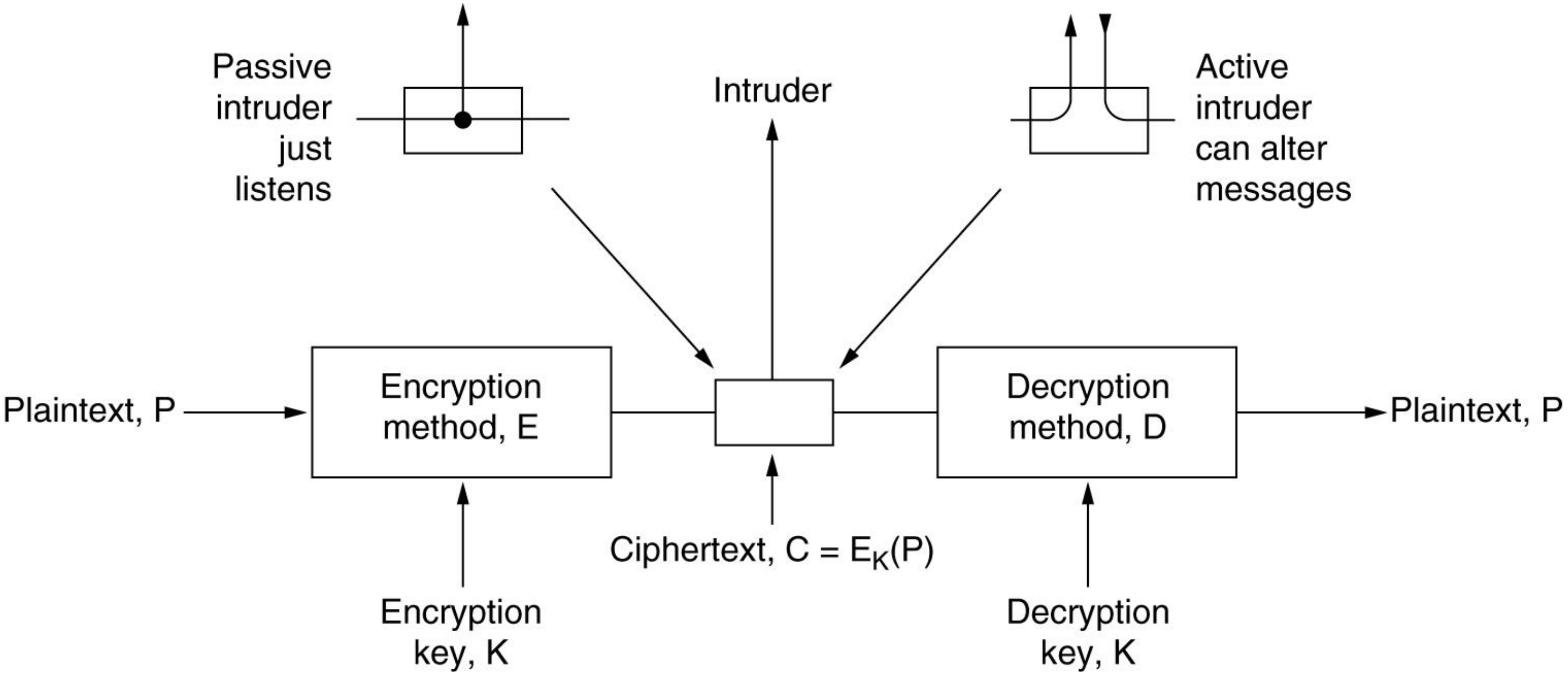
- **Secrecy:** Confidentiality, keeping information out of hands of unauthorized users.
- **Authentication:** Determine whom you are talking to before revealing sensitive information.
- **Non-repudiation:** Deals with signatures. How would you prove that customer placed an order. What if he deny later?
- **Integrity Control:** Finally, how can you be sure that a message you received was really the one sent and not something that a malicious adversary modified at transit?

Except for physical layer security, nearly all network security is based on cryptographic principles.

Cryptography

- **Cryptography** comes from the Greek words for ''secret writing.''‘
- **Encryption + Decryption** = Cryptography.
- **Components involved in cryptography:**
  - **Plaintext**: the original message before being transformed.
  - **Ciphertext**: the coded message after being transformed.
  - **Key**: info used in cipher known only to sender/receiver.

Cryptography Model

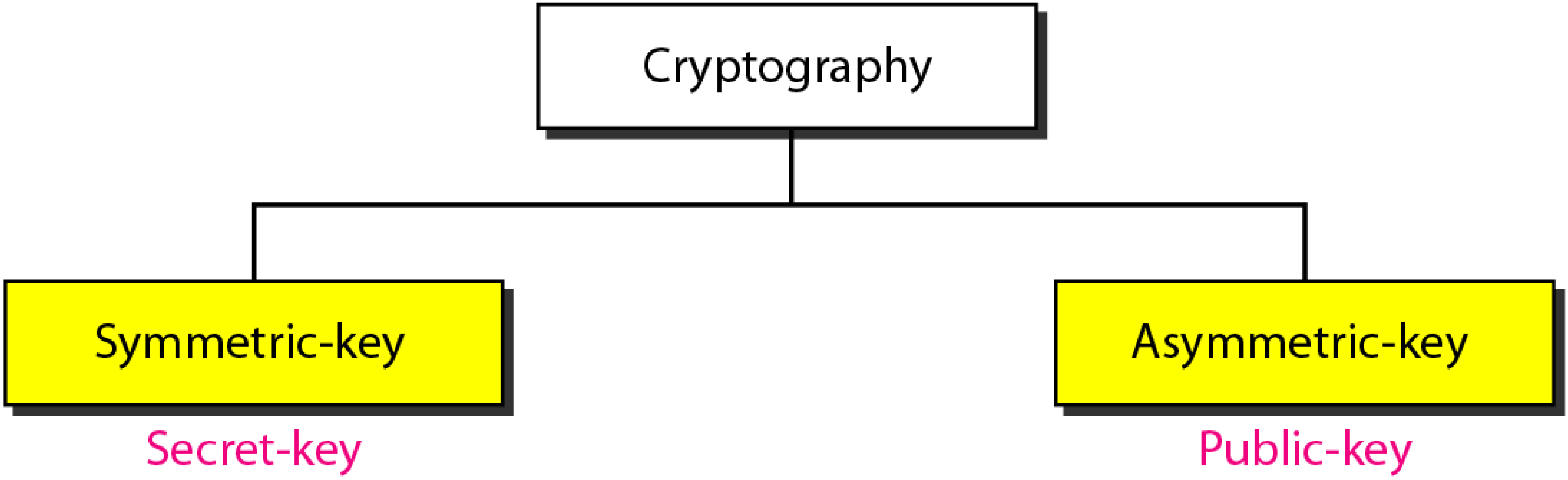


- Relation between plaintext, ciphertext, and keys:
  - $C = E_K(P)$ to mean that the encryption of the plaintext P using key K gives the ciphertext C.
  - $P = D_K(C)$ represents the decryption of C to get the plaintext again.
  - It then follows that $D_K(E_K(P)) = P$

Categories of Cryptography

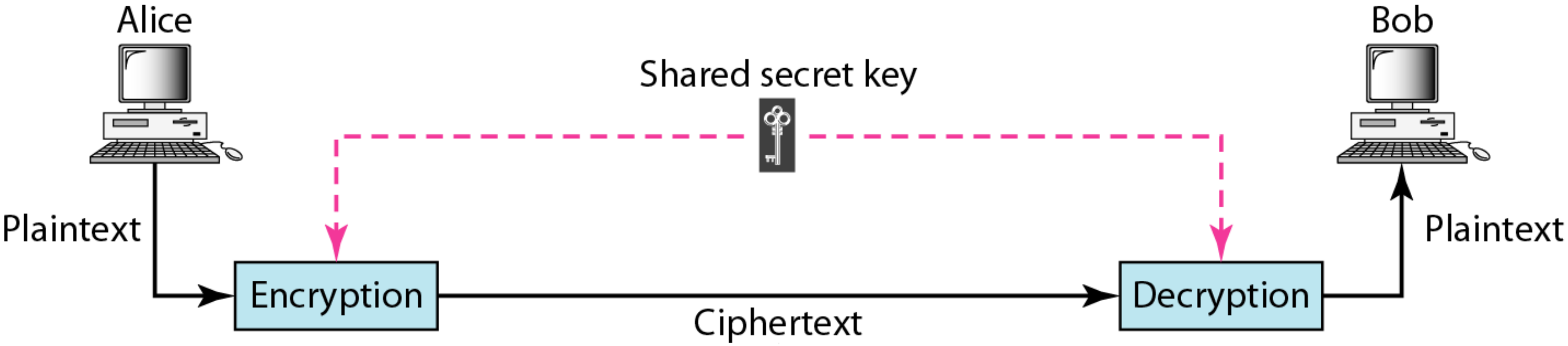
We can divide all the cryptography algorithms into two groups:

- ❖ Symmetric-key (also called secret-key) cryptography algorithms
- ❖ Asymmetric (also called public-key) cryptography algorithms



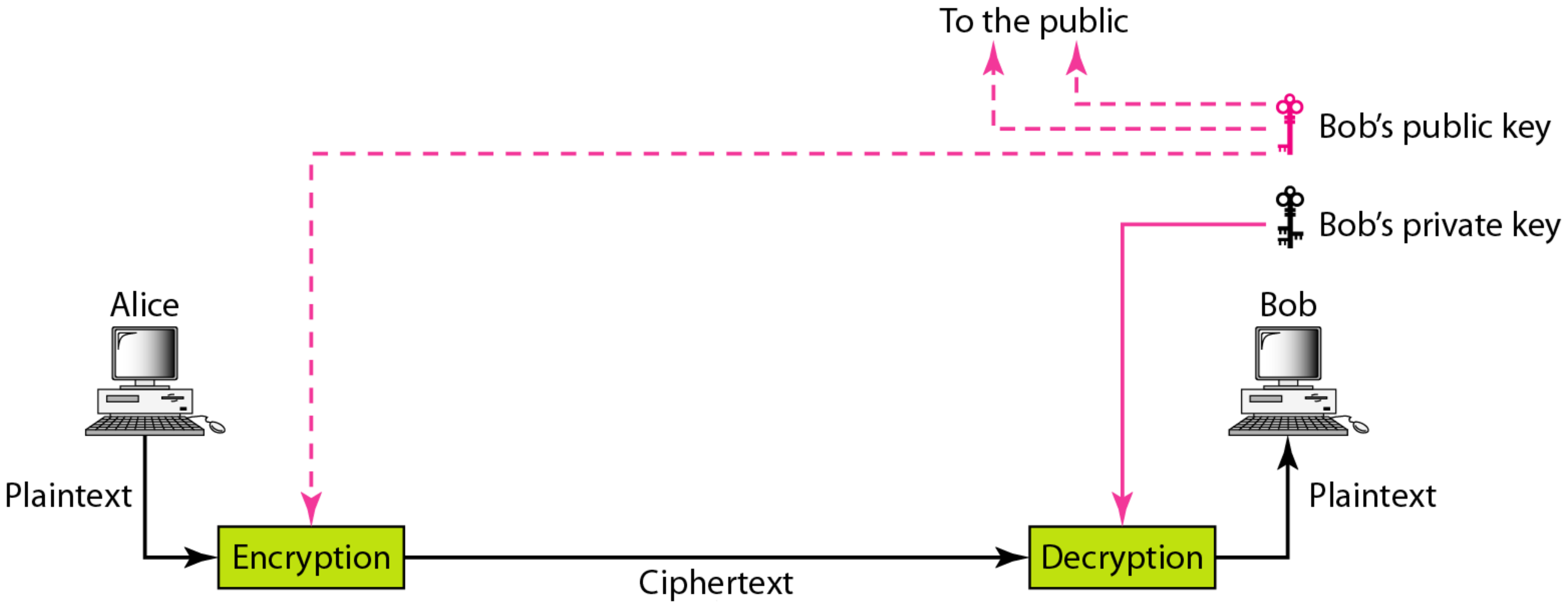
Symmetric-key Cryptography

In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

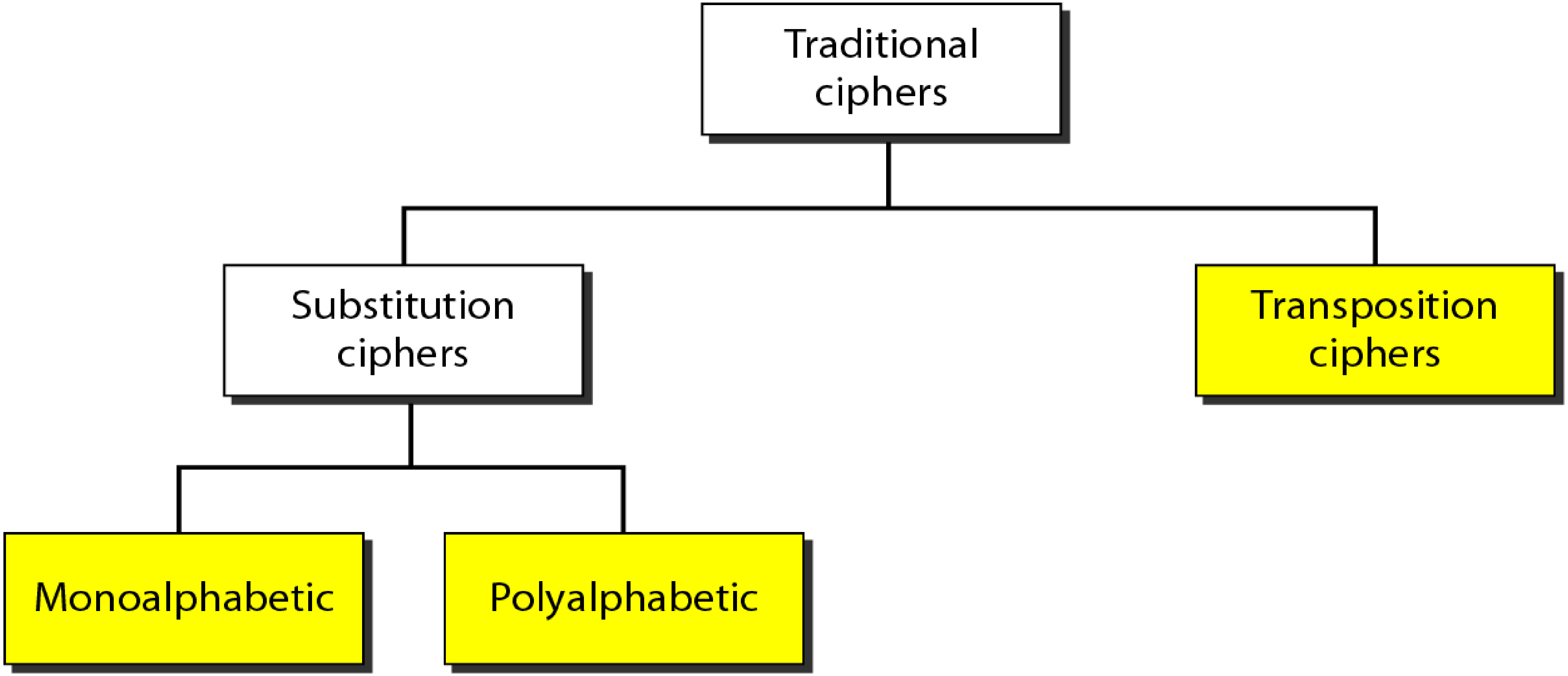


Asymmetric-key Cryptography

In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.



Symmetric-key Cryptography



Substitution Ciphers

- In a substitution cipher, each letter or group of letters is replaced by another letter or group of letters to disguise it.
- **Caesar Cipher**:
  - One of the oldest known ciphers
  - In this method, a becomes D, b becomes E, c becomes F, . . . , and z becomes C.
  - A shift of characters is the general Caesar algorithm.
  - For example, ***attack*** becomes ***DWWDFN.***
- **Disadvantages**
  - Easy to convert to plain text
  - Predictable
  - Can’t fool everyone

Substitution Ciphers

- **Mono-alphabetic Substitution:**
  - The next improvement is to have each of the symbols in the plaintext, say, the 26 letters for simplicity, map onto some other letter.
  - For example,
    - Plaintext:

      a b c d e f g h i j k l m n o p q r s t u v w x y z
    - Ciphertext:

      Q W E R T Y U I O P A S D F G H J K L Z X C V B N M
  - The general system of symbol-for-symbol substitution is called a mono alphabetic substitution
  - key being the 26-letter string corresponding to the full alphabet.
  - 'attack' would be transformed into the cipher text 'QZZQEA'.

Substitution Ciphers

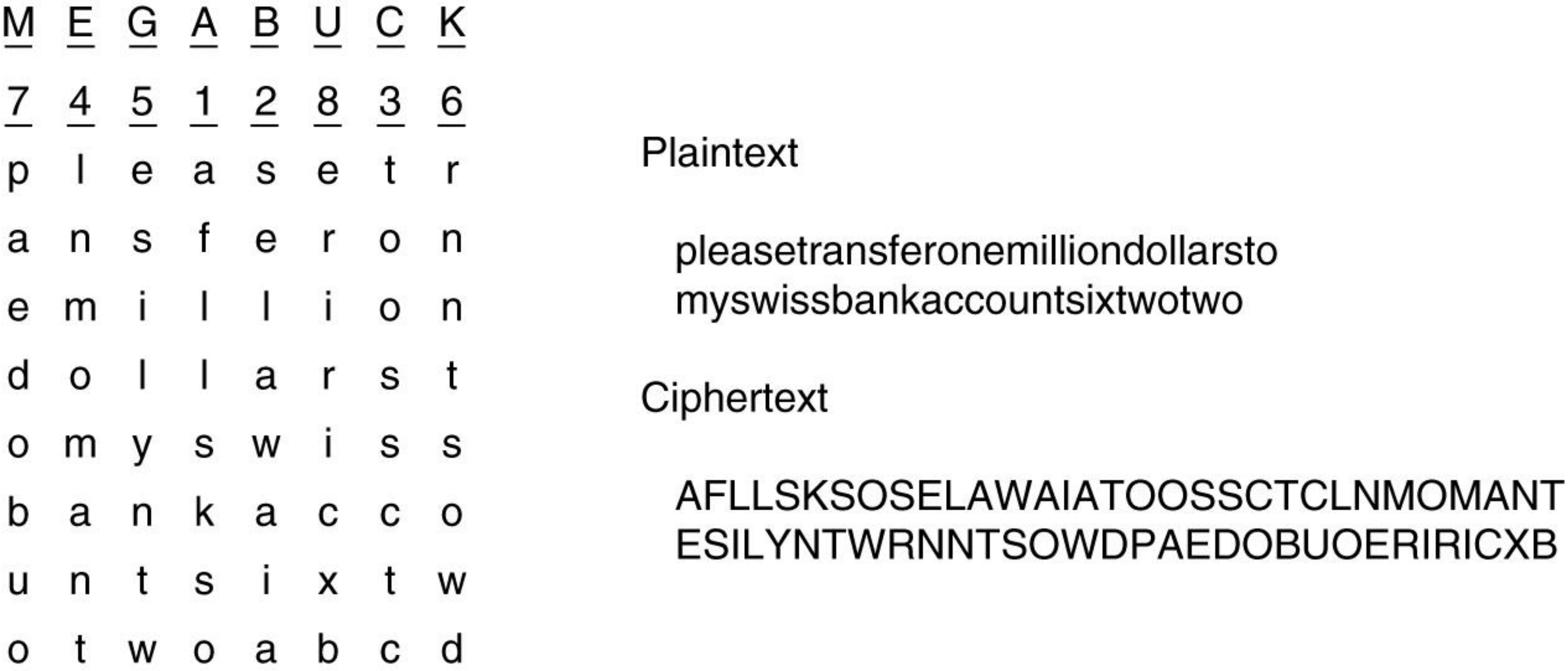
- **Poly-alphabetic Substitution**

  - ❑ A poly-alphabetic cipher is any cipher based on substitution, using several substitution alphabets. In polyalphabetic substitution ciphers, the plaintext letters are enciphered differently based upon their installation in the text. Rather than being a one-to-one correspondence, there is a one-to-many relationship between each letter and its substitutes.
  - ❑ For example, ‘a’ can be enciphered as ‘d’ in the starting of the text, but as ‘n’ at the middle.

Transposition Ciphers

- Transposition cipher reorder the letters but do not disguise them.
- The cipher is keyed by a word or phrase not containing any repeated letters.
- In this example, MEGABUCK is the key.
- The purpose of the key is to number the columns.
- Plaintext is written horizontally, in rows, padded to fill the matrix if need be.
- The cipher text is read out by columns, starting with the column whose key letter is the lowest.
- Every letter represents itself, keeping the frequency distribution intact.

Transposition Ciphers



M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

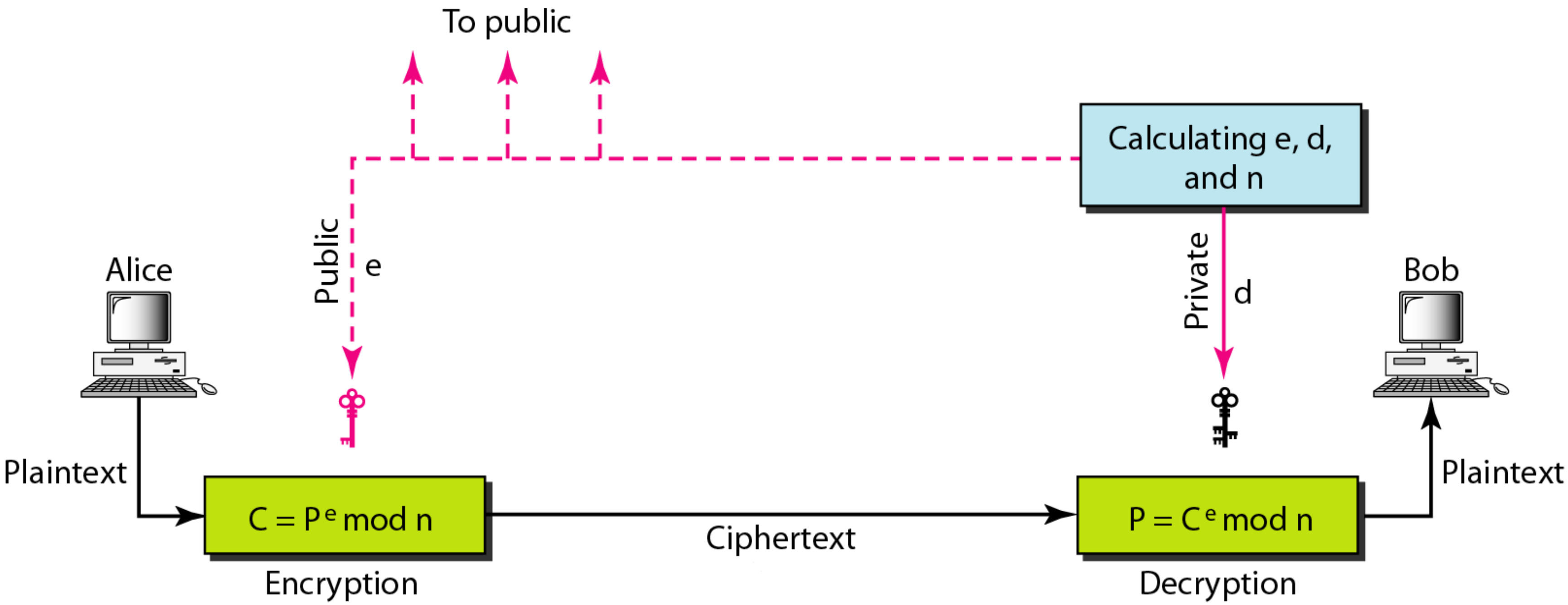
Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

A transposition Cipher

Public-Key Algorithms

- RSA
  - The most common public key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA).
  - It uses two numbers, e and d, as the public and private keys, as shown in Figure



Public-Key Algorithms

- **Selecting Keys:**
  1. Chooses two very large prime numbers $\boldsymbol{p}$ and $\boldsymbol{q}$.
  2. Multiplies the above two primes to find $\boldsymbol{n}$, the modulus for encryption and decryption. In other words, $\boldsymbol{n = p \times q}$.
  3. Calculates another number $\boldsymbol{z = (p - 1) \times (q - 1)}$.
  4. Choose a number, $\boldsymbol{e}$, less than $\boldsymbol{n}$, that has no common factors (other than 1) with $\boldsymbol{z}$. (In this case, $\boldsymbol{e}$ and $\boldsymbol{z}$ are said to be relatively prime.)
  5. Find a number, $\boldsymbol{d}$, such that $\boldsymbol{ed \bmod z = 1}$
  6. Announces $\boldsymbol{e}$ and $\boldsymbol{n}$ to the public; he keeps $\boldsymbol{z}$ and $\boldsymbol{d}$ secret.
- **Encryption:**
  - $C = P^e \pmod{n}$
- **Decryption:**
  - $P = C^d \pmod{n}$