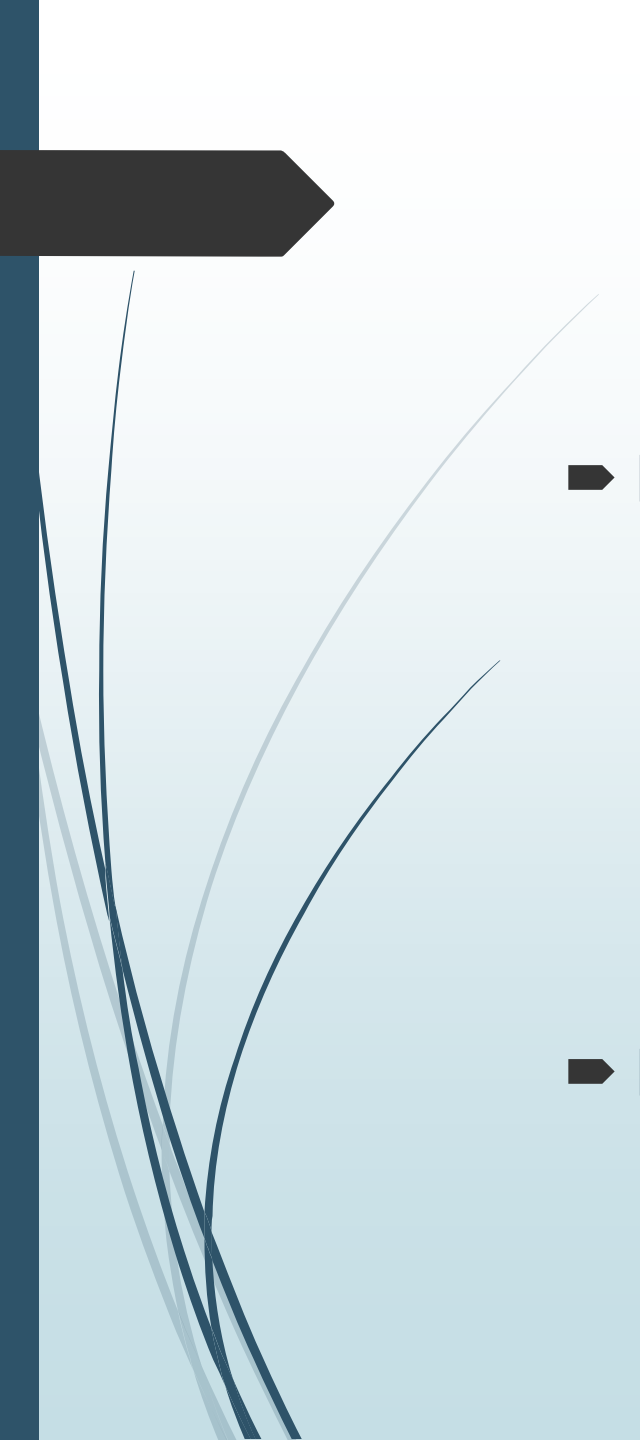



# Principles of Public-Key Cryptosystems

- 
- Evolved from an attempt to solve two of the most difficult problems associated with **symmetric encryption**.
  - Key distribution
  - Digital signature
  - Diffie and Hellman in **1976** came up with a method

- 
- Each user **generates a pair of keys** to be used for the encryption and decryption
  - Each user places one of the two keys in a public register or other accessible file. This is the **public key**
  - The other key is kept private, which is the **private key**
  - Either of the two related keys can be used for encryption, with the other used for decryption.



# A public-key encryption scheme has six ingredients

- Plaintext
- Encryption algorithm
- Public key
- Private key
- Cipher text
- Decryption algorithm

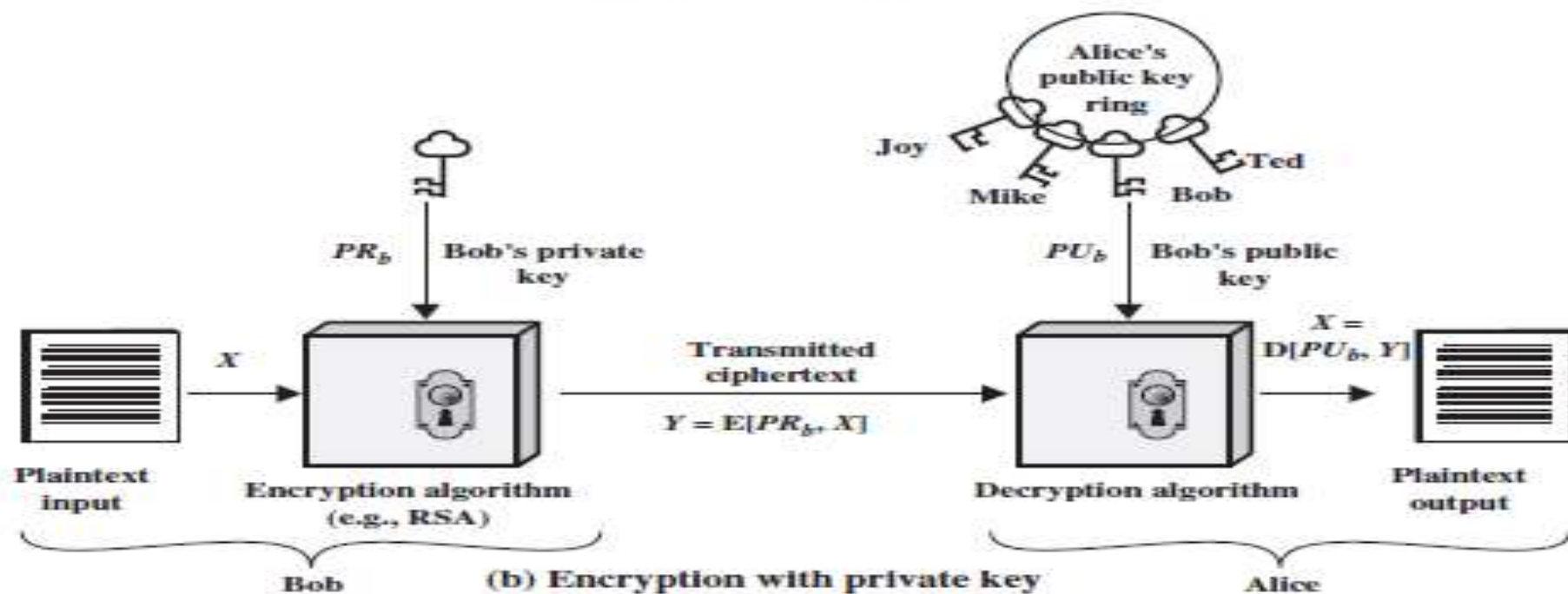
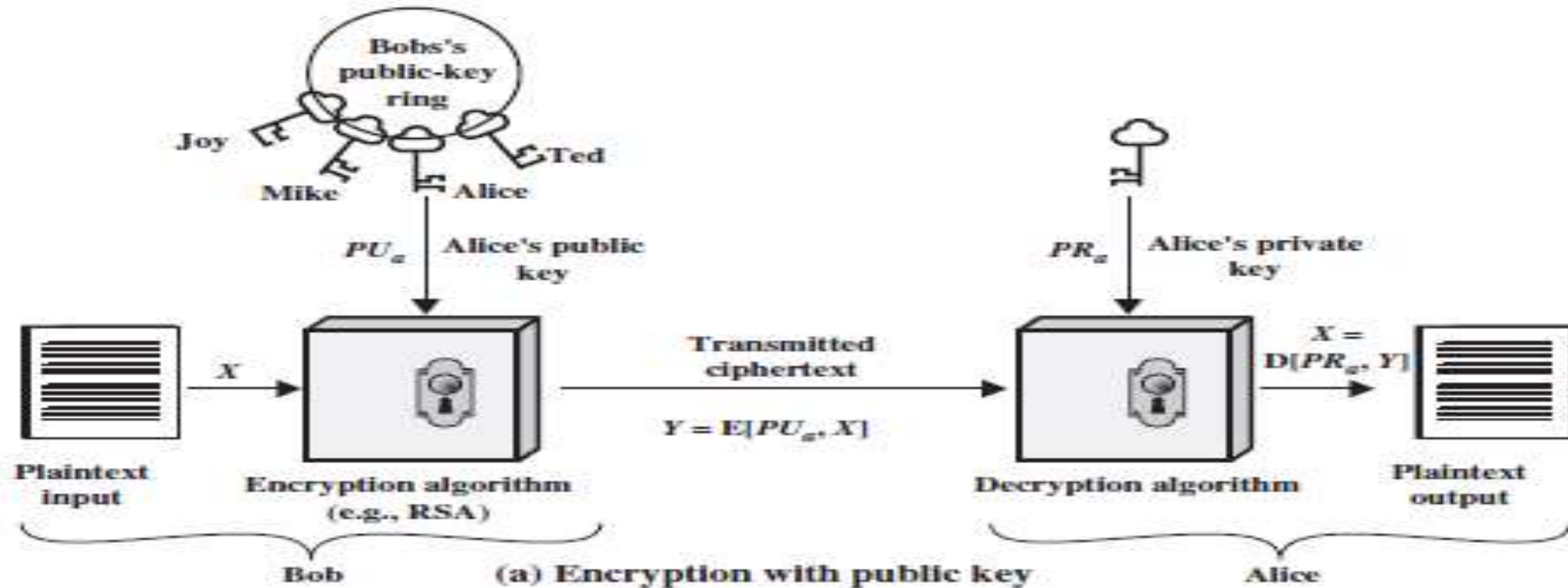


Figure 9.1 Public-Key Cryptography

# Encryption using Public key

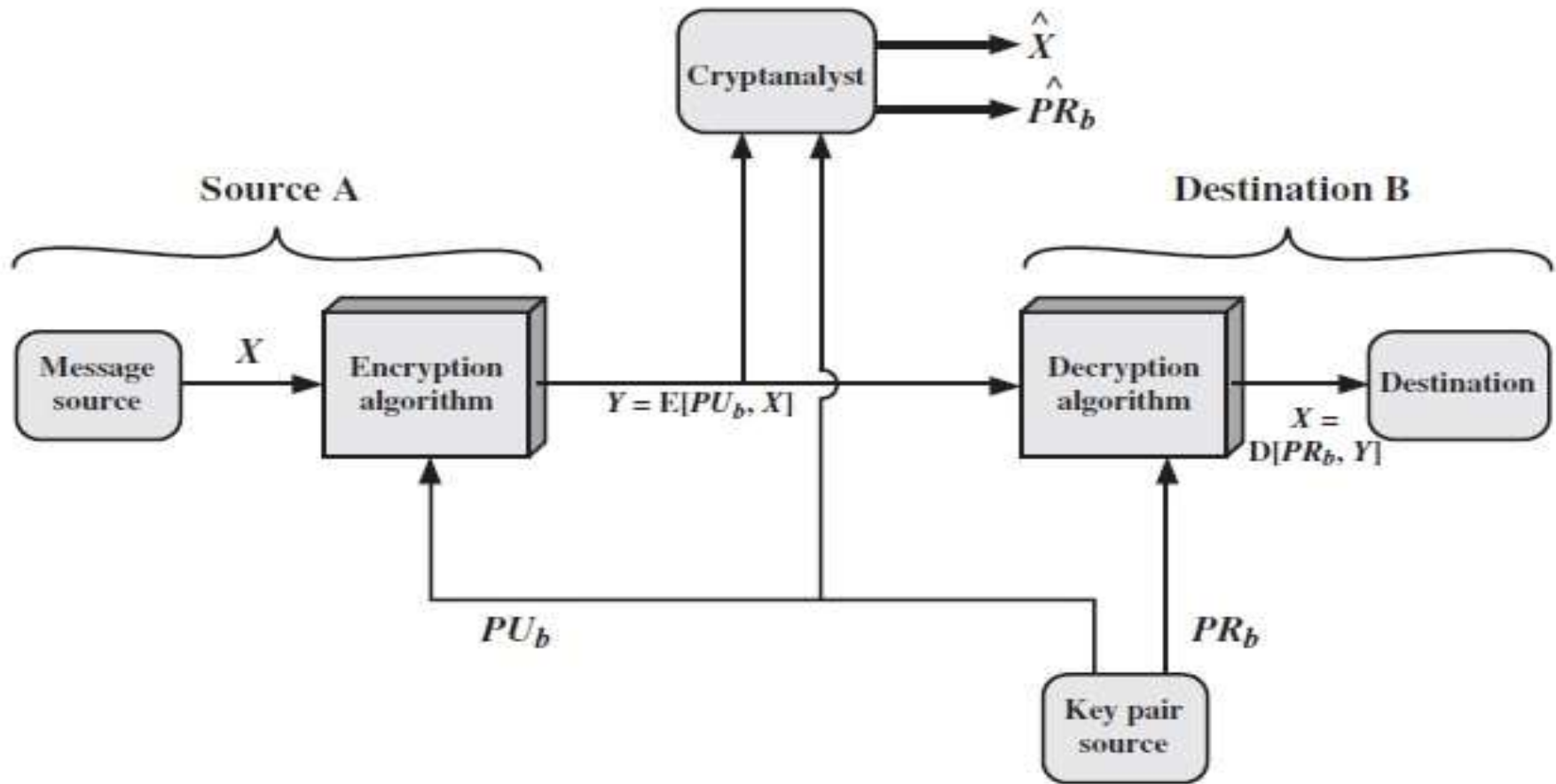


Figure 9.2 Public-Key Cryptosystem: Secrecy



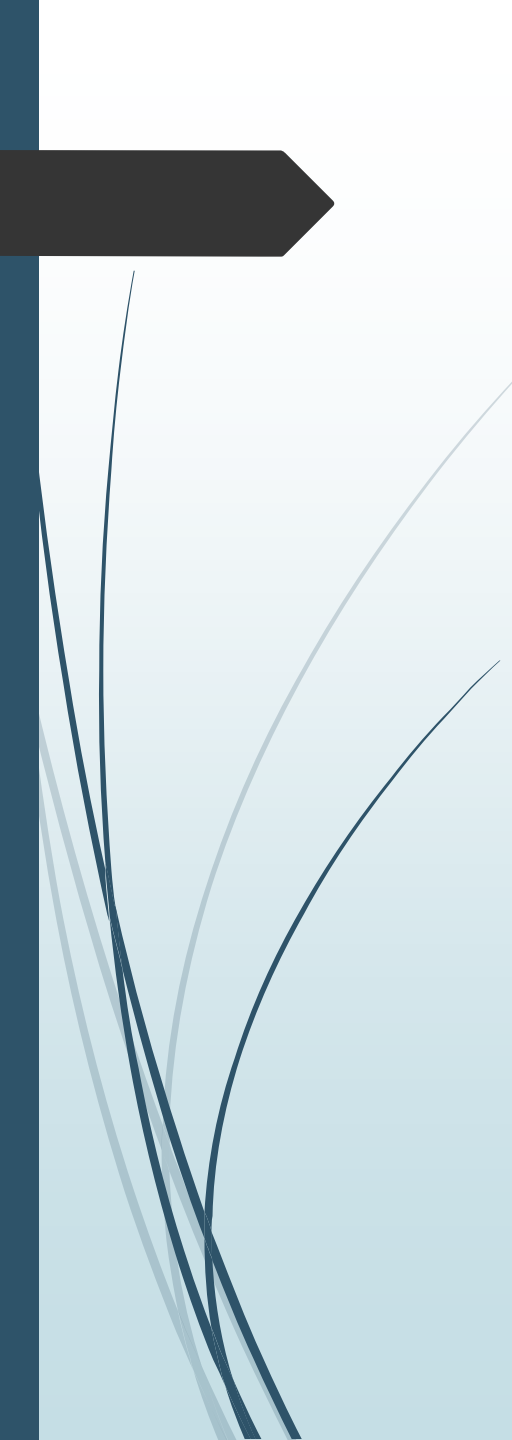
➤ With the **message**  $X$  and the **encryption key**  $PUB$  as input

➤ A forms the **ciphertext**  $Y$  , given by

$$➤ Y = E(PUB, X)$$

➤ Receiver in possession of the matching private key  $PRb$ , is able to invert the transformation

$$➤ X = D(PRb, Y)$$

- 
- An **adversary**, observing  $Y$  and having access to  $PUB$ , but not having access to  $PRb$  or  $X$ , must attempt to recover  $X$  and/or  $PRb$ .
  - It is assumed that the adversary does **have knowledge** of the encryption (E) and decryption (D) **algorithms**.
  - If the adversary is interested only in this **particular message**, then the focus of effort is to recover  $X$  by generating a plaintext estimate  $X_n$ .
  - Often, however, the adversary is interested in being able to read **future messages as well**, in which case an attempt is made to recover  $PRb$  by generating an **estimate**  $PRnb$ .



# Encryption using Private key

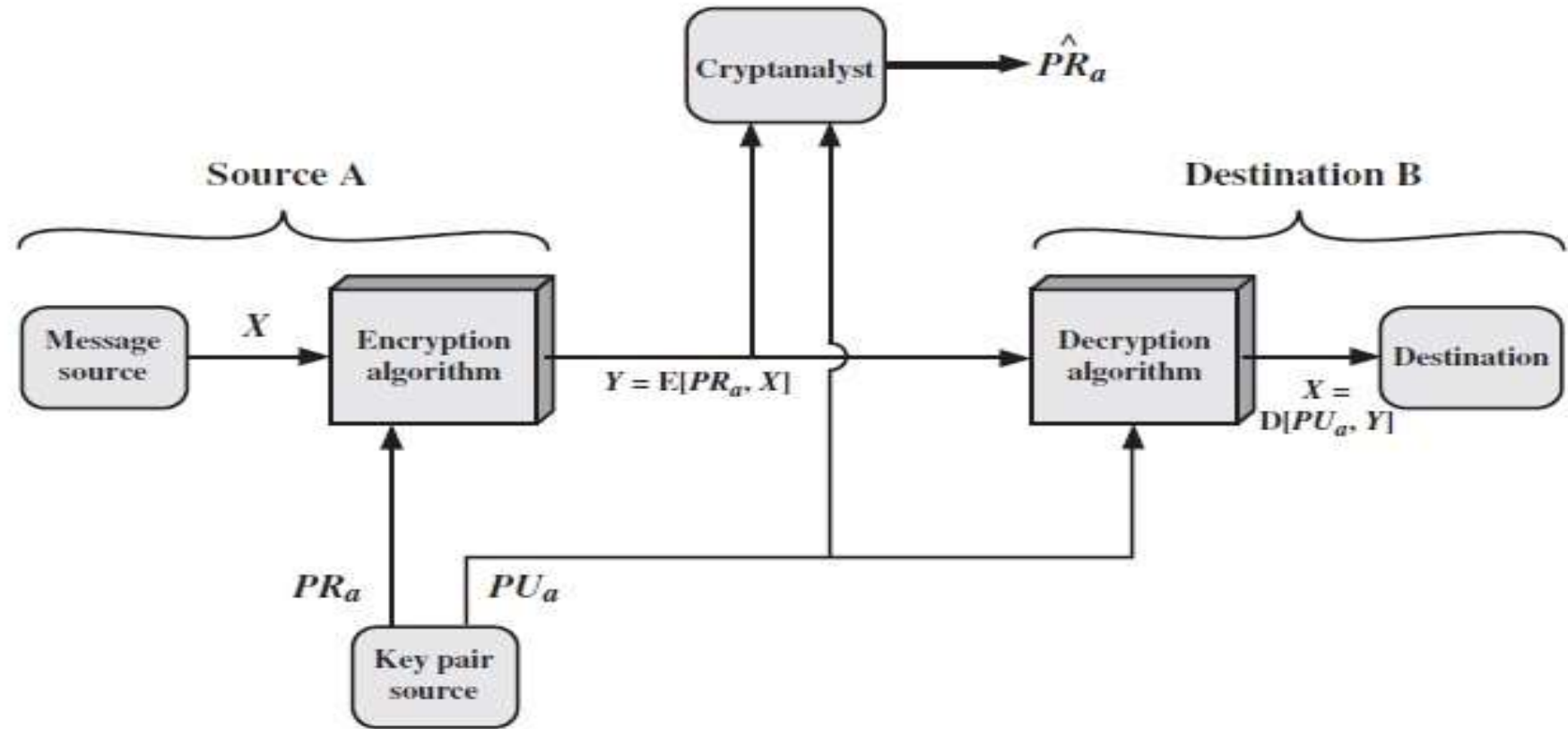




Figure 9.3 Public-Key Cryptosystem: Authentication

- 
- A encrypts it using A's private key before transmitting it.
  - B can decrypt the message using A's public key.
    - $Y = E(PR_a, X)$
    - $X = D(PU_a, Y)$
  - Only A could have prepared the message, Therefore, the entire encrypted message serves as a **digital signature**.

- 
- In addition, it is **impossible to alter** the message without access to A's private key
  - The message being sent is **safe from alteration**.
  - But **not confidentiality** because any observer can decrypt the message by using the sender's public key.

# Authentication and confidentiality

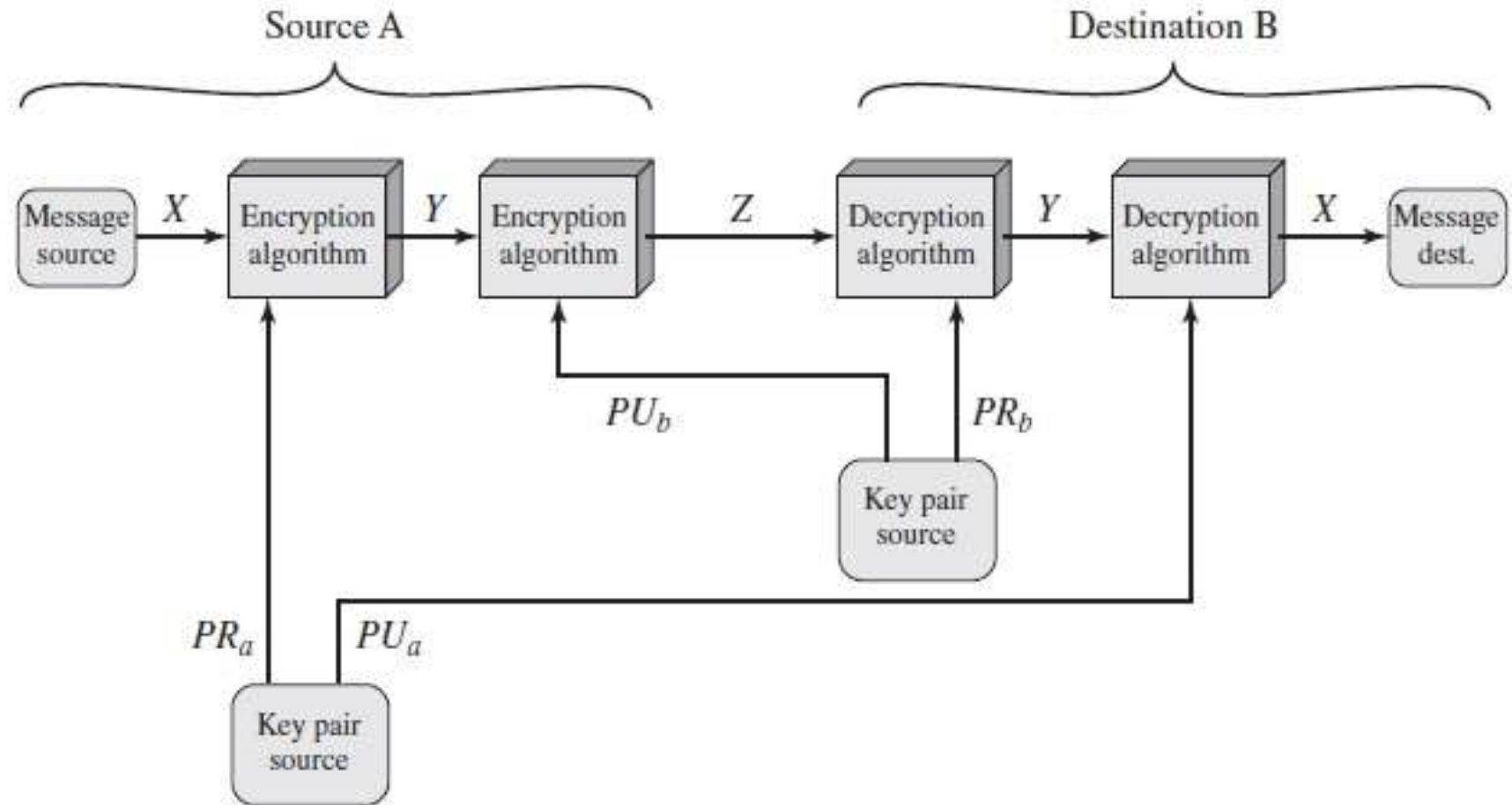




Figure 9.4 Public-Key Cryptosystem: Authentication and Secrecy

- 
- Both the authentication function and confidentiality by a double use of the public-key scheme

- $Z = E(PUb, E(PRa, X))$

- $X = D(PUa, D(PRb, Z))$

- 
- We begin by encrypting a message, using the sender's private key.
  - This provides the **digital signature**.
  - Next, we encrypt again, using the receiver's public key.
  - The final ciphertext can be decrypted only by the intended receiver, who alone has the matching private key.
  - Thus, **confidentiality** is provided.



# Applications for Public-Key Cryptosystems

- Encryption/decryption
- Digital signature
- Key exchange
- Some algorithms are suitable for all three applications,
- Some used only for one or two of these applications.

# Requirements for Public-Key Cryptography

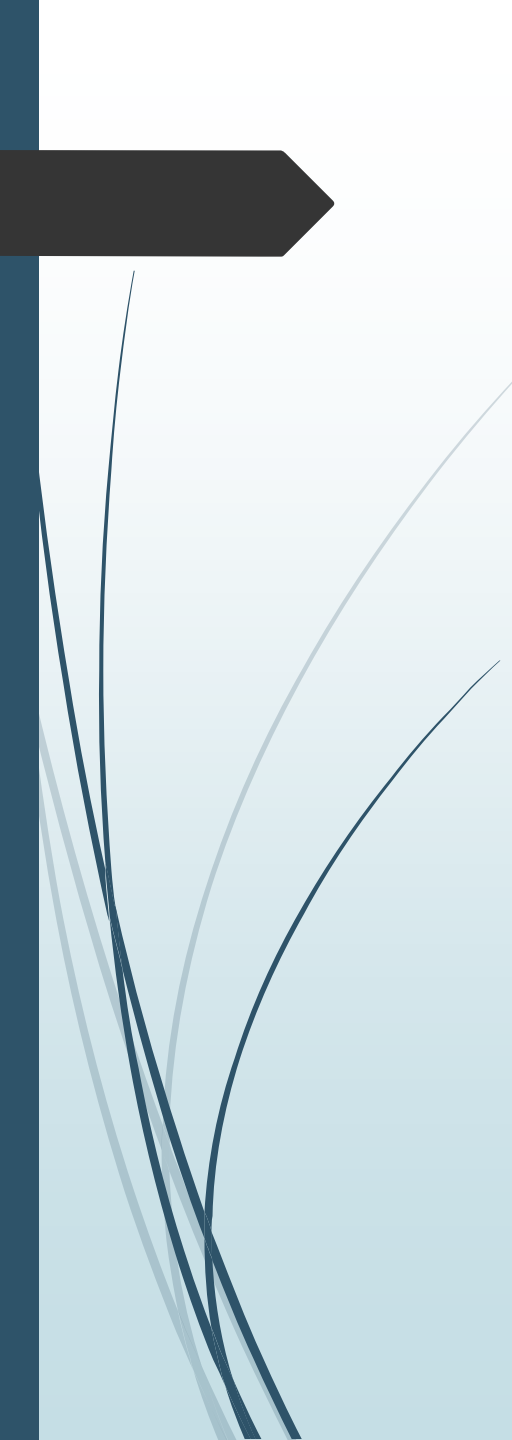
- 1. It is computationally easy for a party B to generate a pair of key (public key  $PUB$ , private key  $PRb$ ).
- 2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted,  $M$ , to generate the corresponding ciphertext:

$$➤ C = E(PUB, M)$$

- 3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message:

$$➤ M = D(PRb, C) = D[PRb, E(PUB, M)]$$



- 
- 4. It is computationally infeasible for an adversary, knowing the public key,  $PUB$ , to determine the private key,  $PRb$ .
  - 5. It is computationally infeasible for an adversary, knowing the public key,  $PUB$ , and a ciphertext,  $C$ , to recover the original message,  $M$
  - 6. The two keys can be applied in either order:
    - $M = D[PUB, E(PRb, M)] = D[PRb, E(PUB, M)]$



# Public-Key Cryptanalysis

- Vulnerable to a brute-force attack.
- The countermeasure is the same: Use large keys.
- Key size must be large enough to make brute-force attack impractical but small enough for practical encryption and decryption.

A decorative graphic on the left side of the slide. It features a dark blue vertical bar on the far left. To its right, there is a dark blue arrow pointing right, positioned in the upper left quadrant. Below the arrow, several thin, dark blue curved lines sweep upwards and to the right, creating a sense of movement or a stylized plant. The background of the slide is a light blue gradient.

thank you