Public key Cryptography

- **Public key cryptography** (PKC) is an **encryption** technique that uses a paired **public** and private **key** algorithm for secure data communication.
- A message sender uses a recipient's **public key** to encrypt a message.
- To decrypt the sender's message, only the recipient's **private key** may be used.

Principles of Public-Key Cryptosystems

- The concept of public-key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption:

Principles of Public-Key Cryptosystems

Key distribution

- The communicants already shares a key or someone has been distributed the key.
- How to secure communications in general without having to trust a KDC with your key

Digital signatures

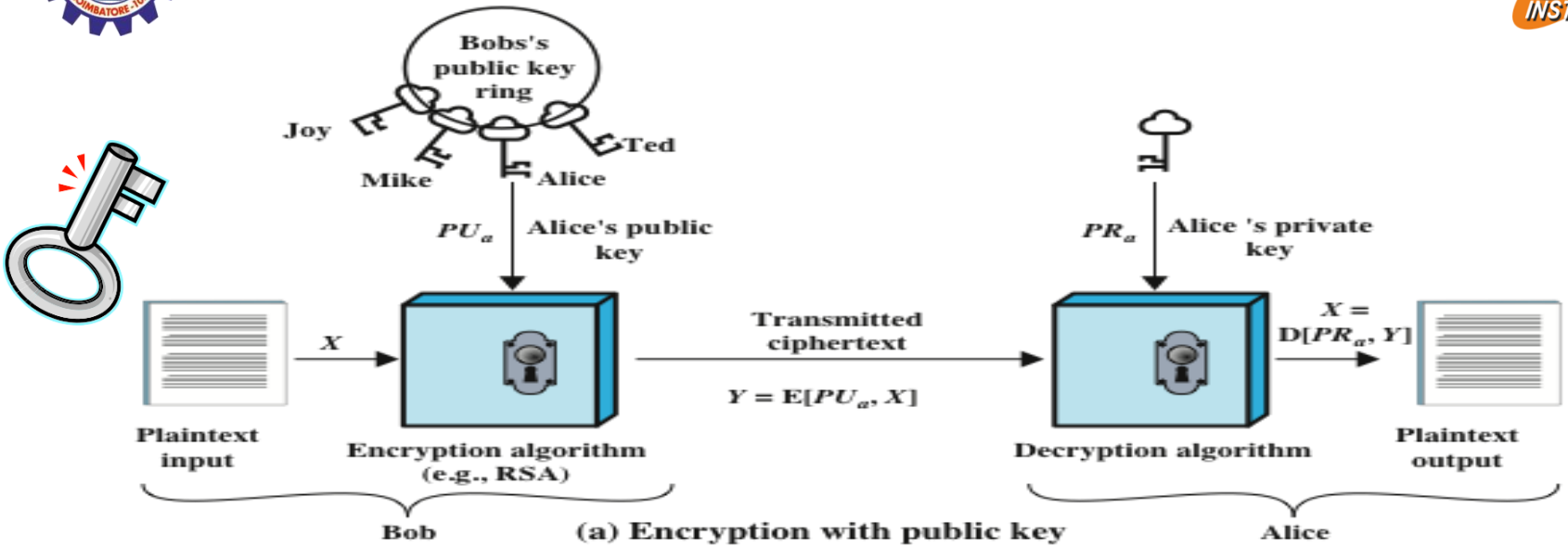
- How to verify that a message comes intact from the claimed sender

Principles of Public-Key Cryptosystems

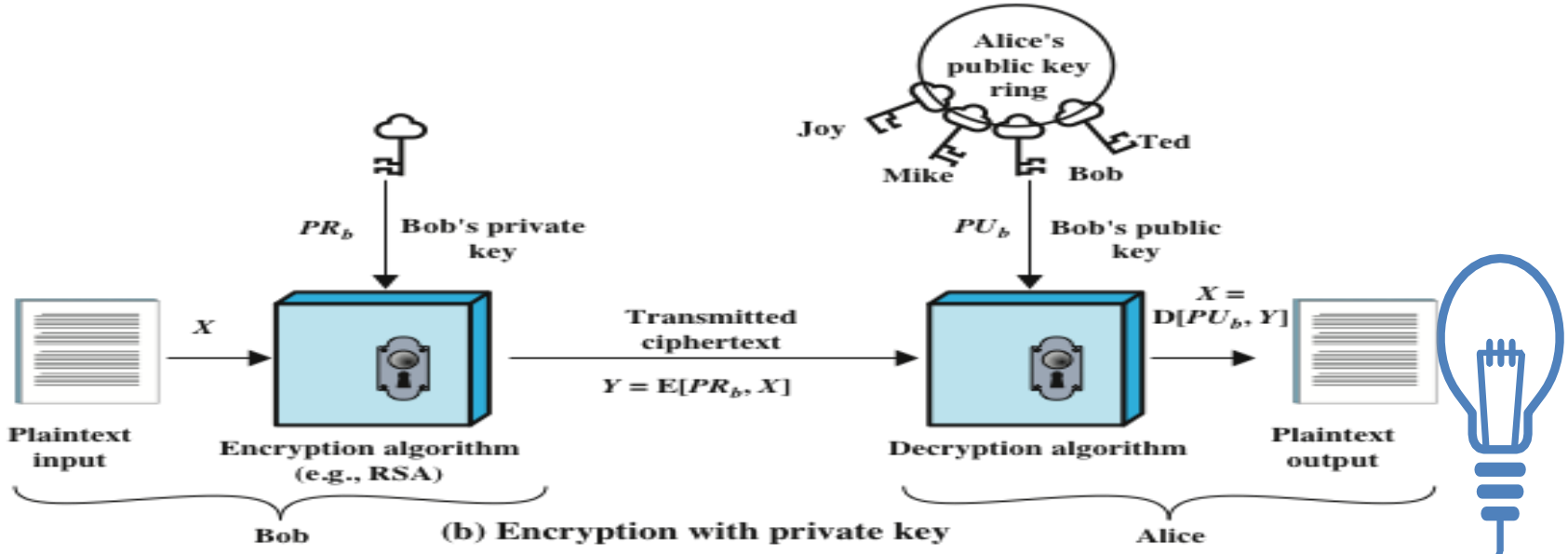
A public-key encryption scheme has six ingredients

Plaintext	Encryption algorithm	Public key	Private key	Ciphertext	Decryption algorithm
The readable message or data that is fed into the algorithm as input	Performs various transform-ations on the plaintext	Used for encryption or decryption	Used for encryption or decryption	The scrambled message produced as output	Accepts the ciphertext and the matching key and produces the original plaintext

Principles of Public-Key Cryptosystems



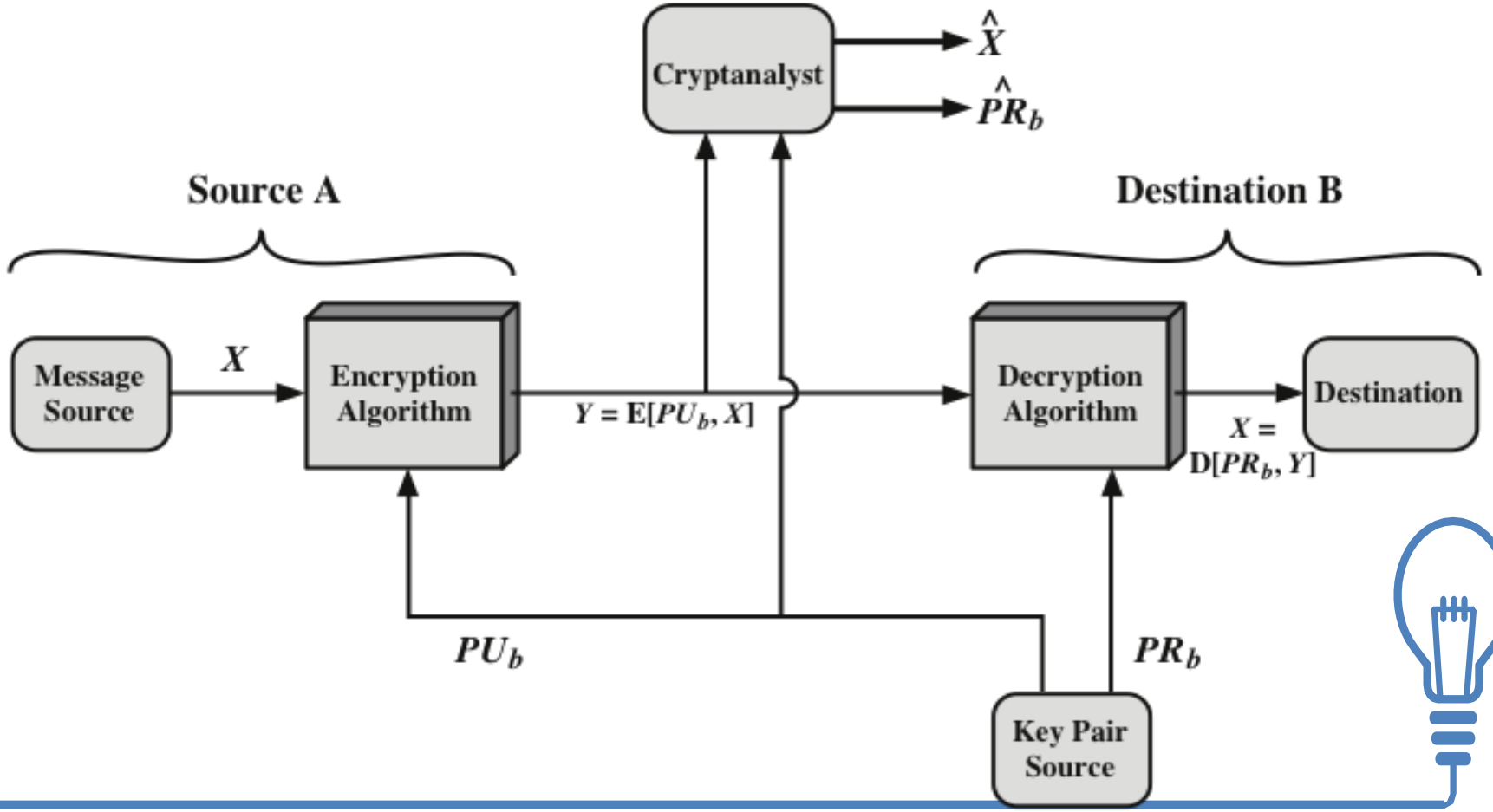
(a) Encryption with public key



(b) Encryption with private key

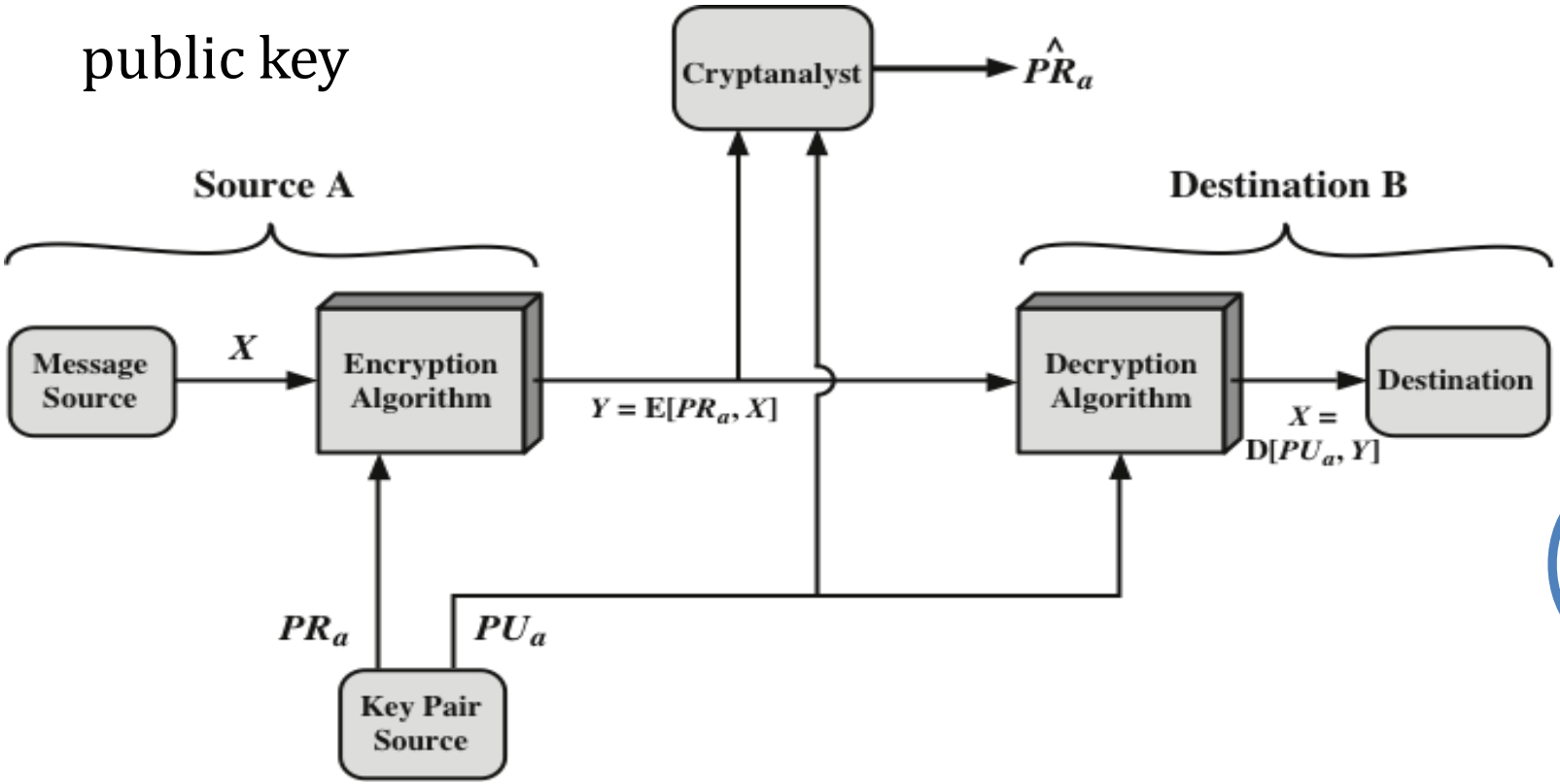
Public-Key Cryptosystem: Encryption using public key -Secrecy

This figure provides confidentiality because two related key used for encryption other being used for decryption



Public-Key Cryptosystem: Encryption using private key -Authentication

There is no protection of confidentiality because any observer can decrypt the message by using the sender's public key

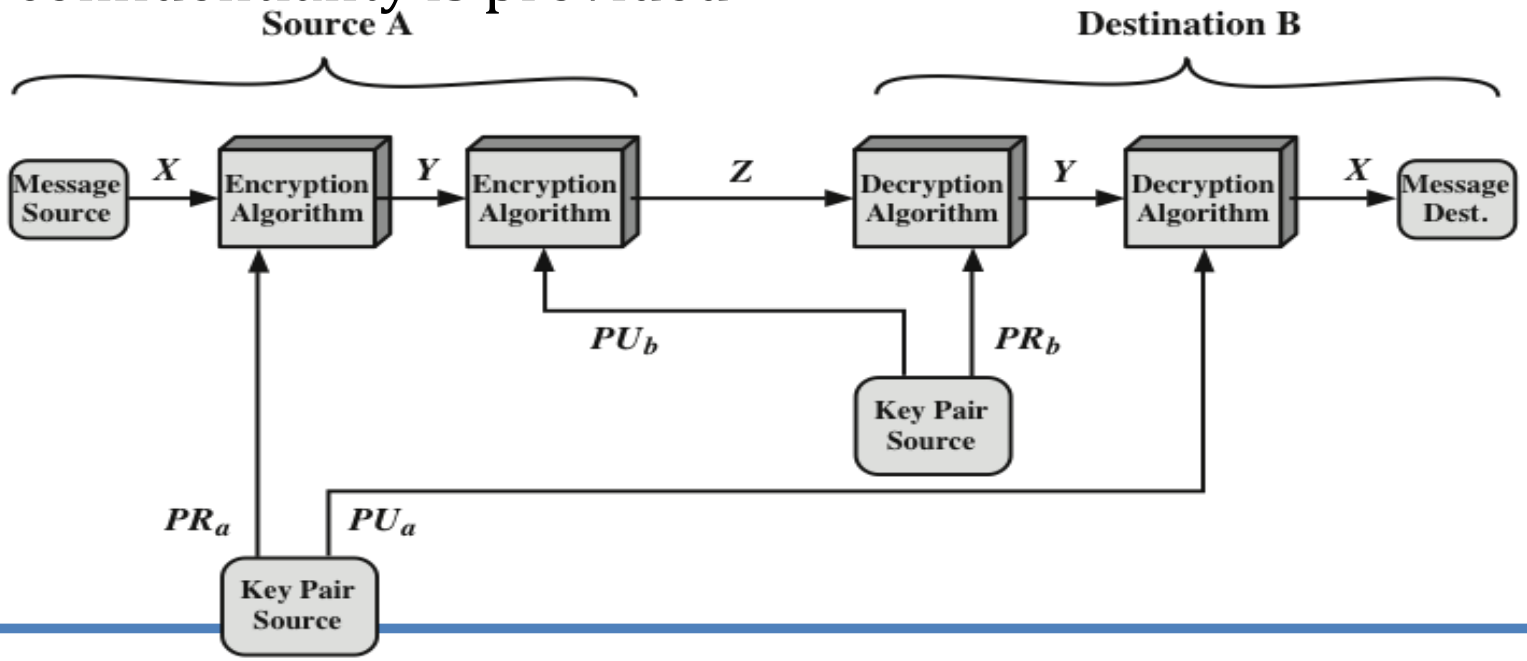


Public-Key Cryptosystem: Authentication and Secrecy

Encrypting a message, using the sender's private key. This provides the digital signature.

Next, 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

- Public-key cryptosystems can be classified into three

Encryption/decryption	• The sender encrypts a message with the recipient's public key
Digital signature	• The sender "signs" a message with its private key
Key exchange	• Two sides cooperate to exchange a session key