Information & System Security

Lecture 28

VIT-AP
UNIVERSITY

Asymmetric

or

Public Key

Cryptography

10-1 INTRODUCTION

Symmetric and asymmetric-key cryptography will exist in parallel and continue to serve the community. We actually believe that they are complements of each other; the advantages of one can compensate for the disadvantages of the other.

Topics discussed in this section:

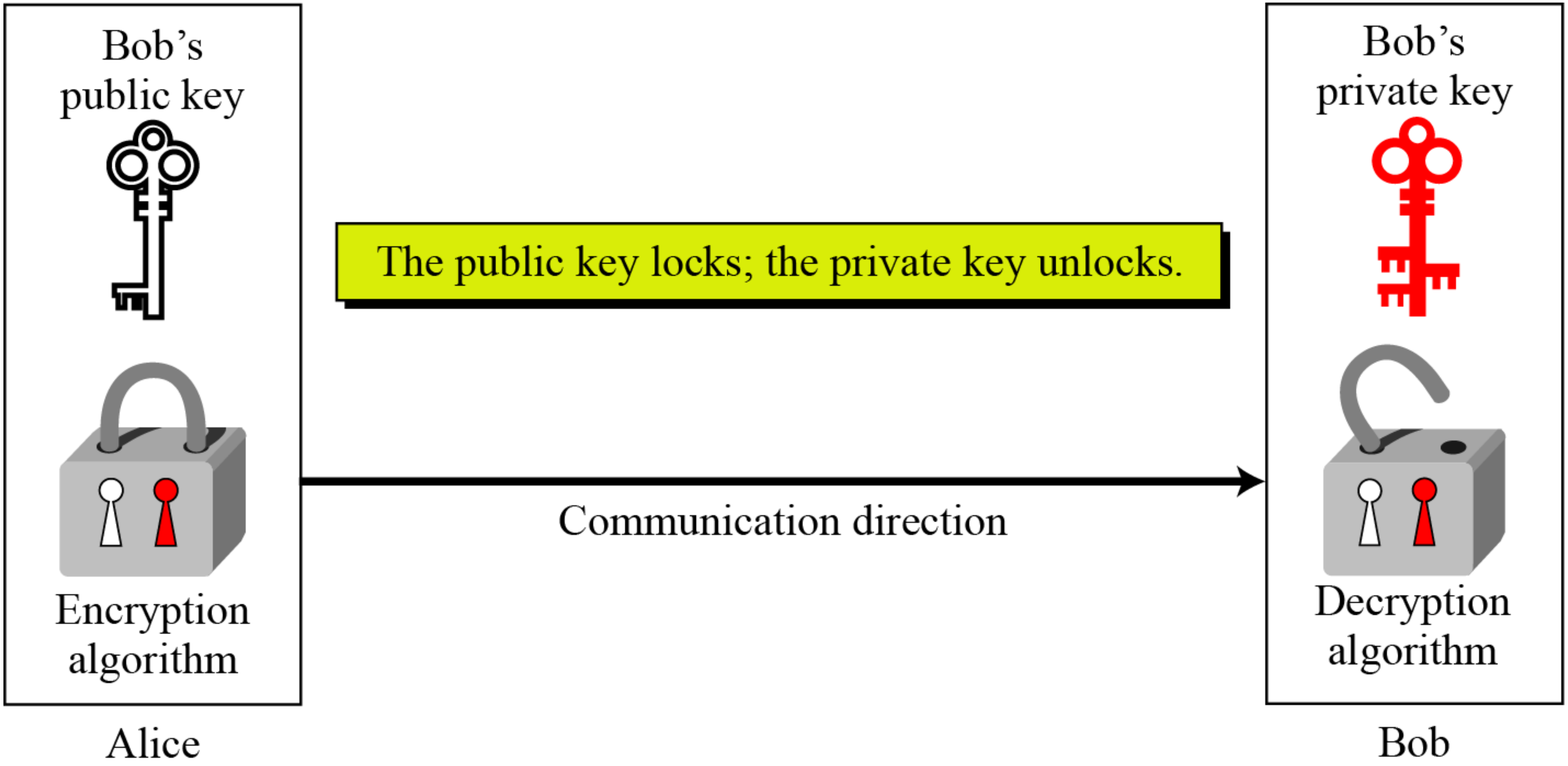
10.1.1 Keys
10.1.2 General Idea
10.1.3 Need for Both

Note

Symmetric-key cryptography is based on sharing secrecy; asymmetric-key cryptography is based on personal secrecy.

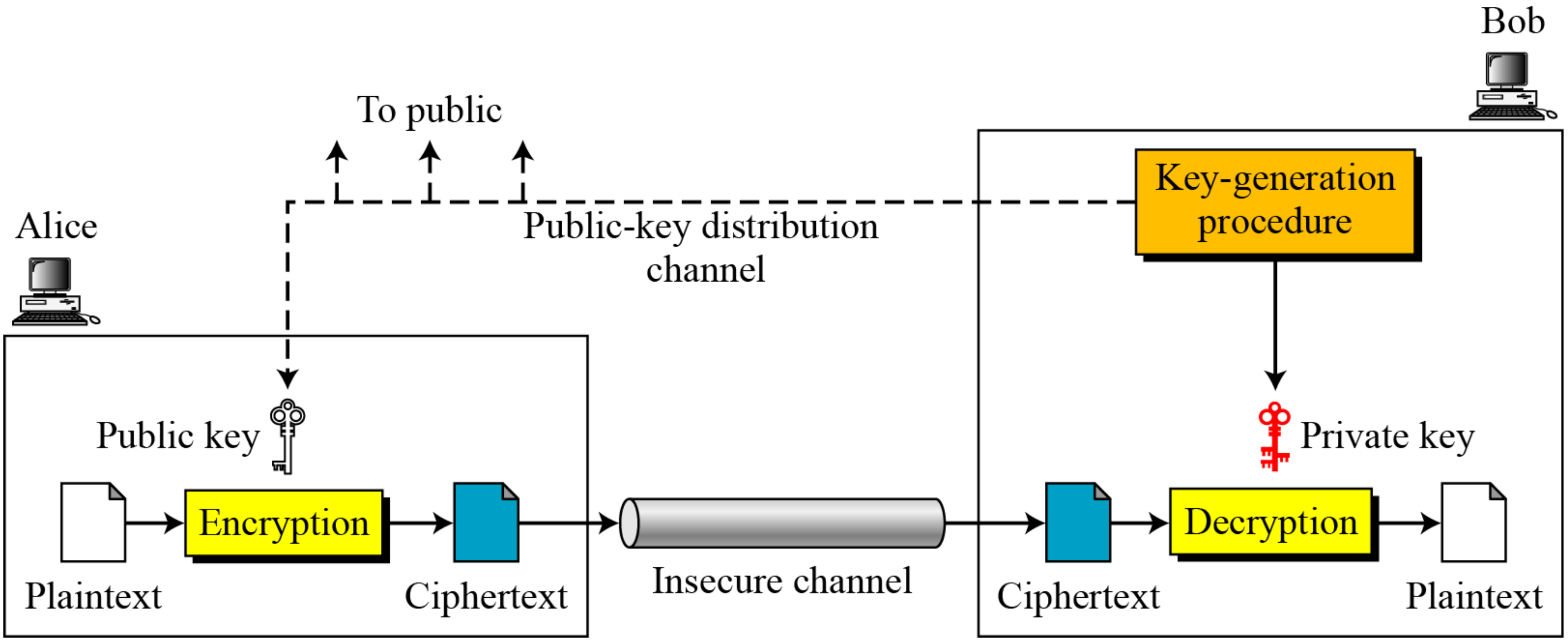
10.1.1 Keys

Asymmetric key cryptography uses two separate keys: one private and one public.



Locking and unlocking in asymmetric-key cryptosystem

10.1.2 General Idea



General idea of asymmetric-key cryptosystem

10.1.2 Continued

Plaintext/Ciphertext

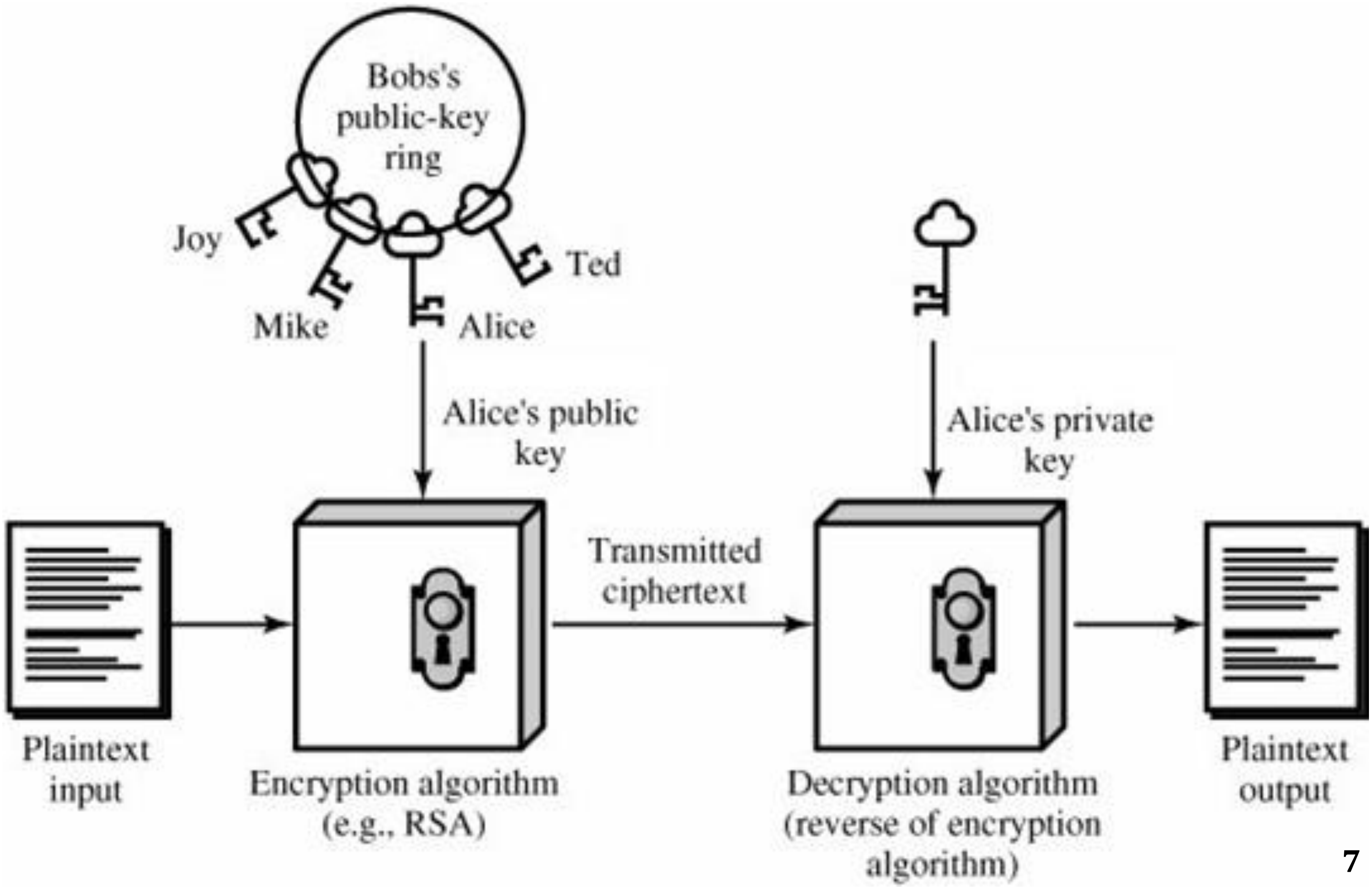
Unlike in symmetric-key cryptography, plaintext and ciphertext are treated as integers in asymmetric-key cryptography.

Encryption $\boxed{C = E(K_{public}, P)}$

Decryption $\boxed{P = D(K_{private}, C)}$

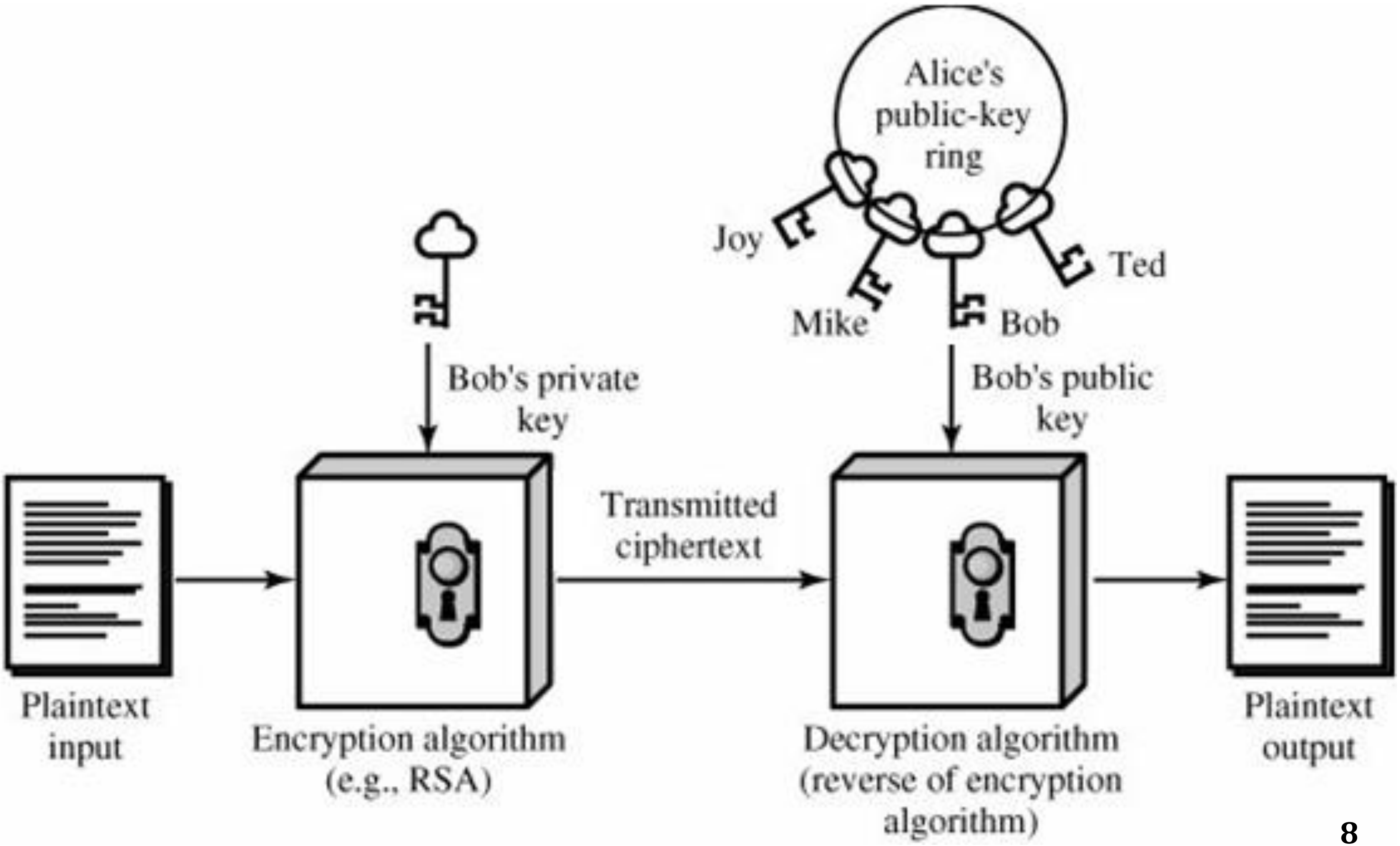
10.1.2 Continued

PKC for Encryption



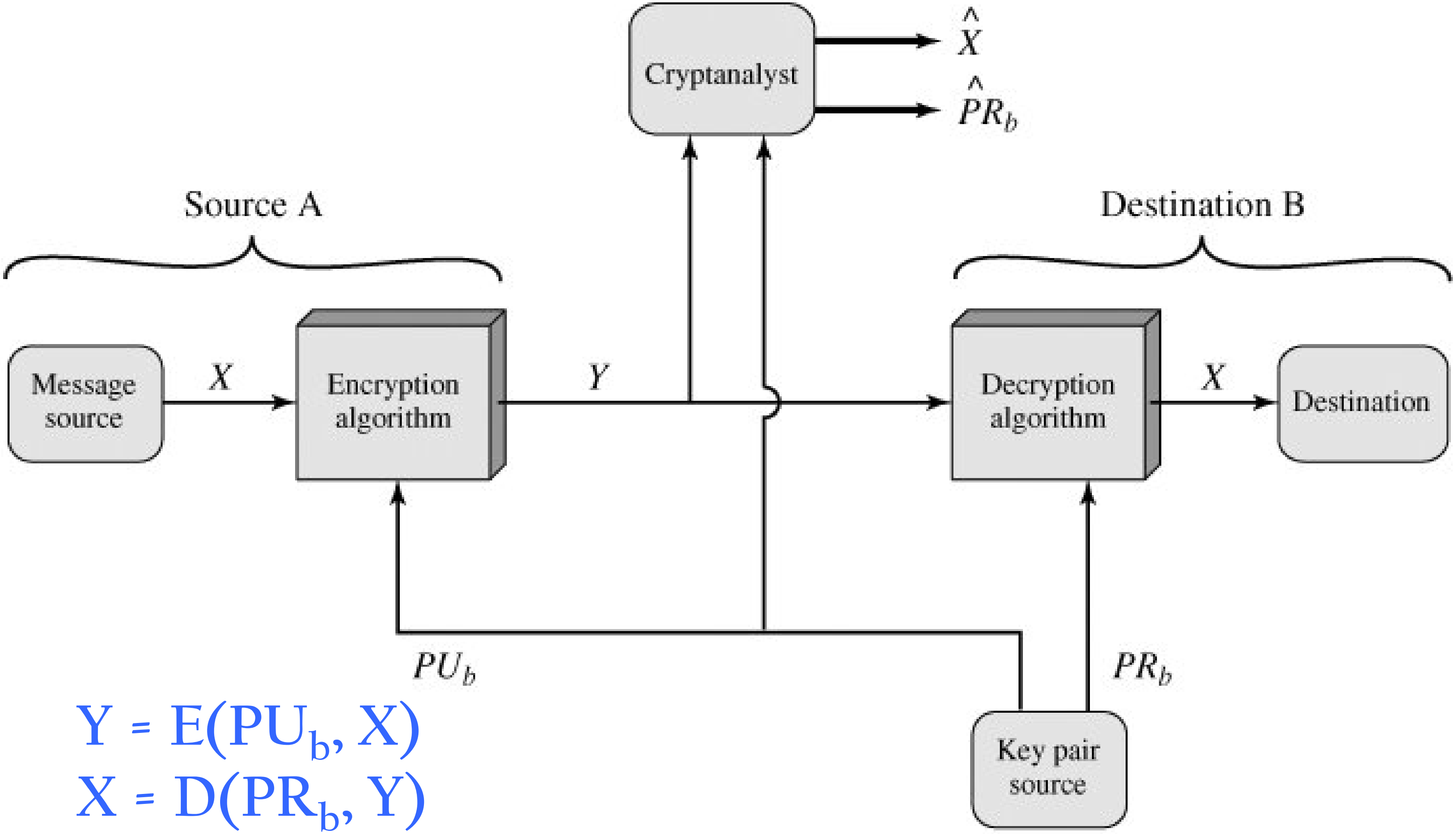
10.1.2 Continued

PKC for Authentication



10.1.2 Continued

PKC for Secrecy

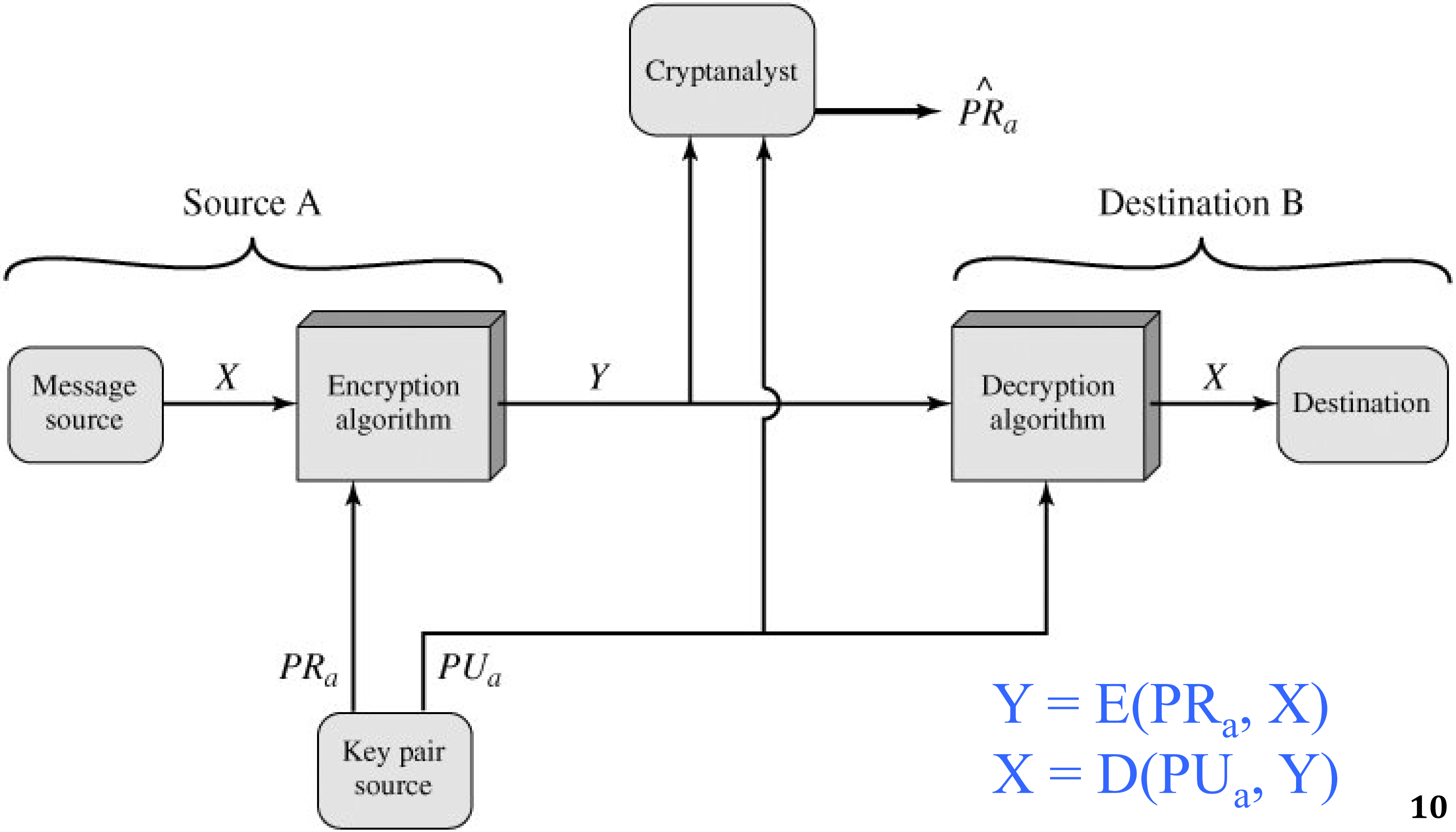


$Y = E(PU_b, X)$

$X = D(PR_b, Y)$

10.1.2 Continued

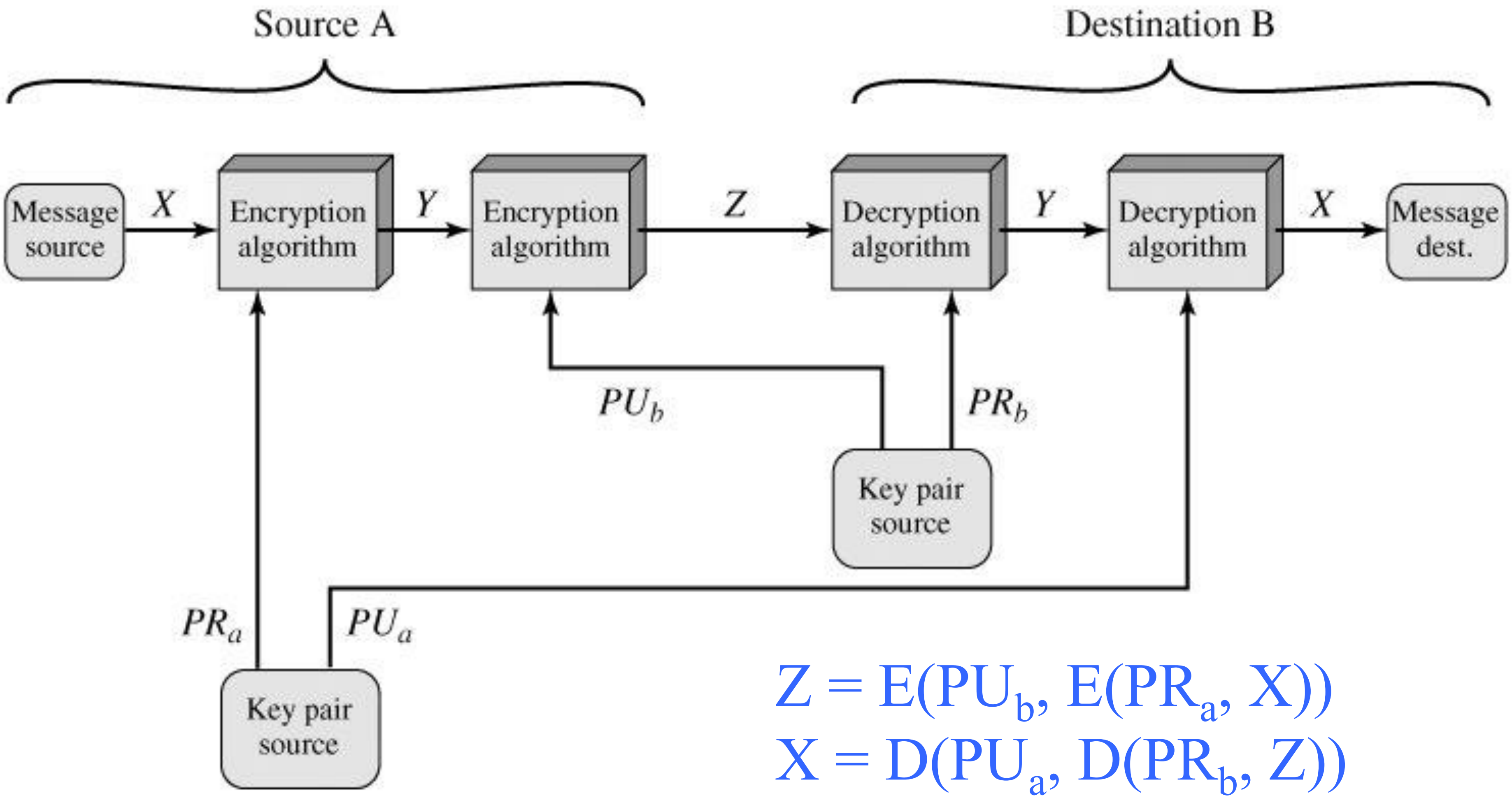
PKC for Authentication



$$Y = E(PR_a, X)$$
$$X = D(PU_a, Y)$$

10.1.2 Continued

PKC for both Authentication & Secrecy



$$Z = E(PU_b, E(PR_a, X))$$

$$X = D(PU_a, D(PR_b, Z))$$

10.1.2 Continued

Symmetric and Asymmetric-Key Encryption

Symmetric-Key Encryption

Needed to Work:

1. The same algorithm with the same key is used for encryption and decryption.
2. The sender and receiver must share the algorithm and the key.

Needed for Security:

1. The key must be kept secret.
2. It must be impossible or at least impractical to decipher a message if no other information is available.
3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.

Asymmetric-Key Encryption

Needed to Work:

1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
2. The sender and receiver must each have one of the matched pair of keys (not the same one).

Needed for Security:

1. One of the two keys must be kept secret.
2. It must be impossible or at least impractical to decipher a message if no other information is available.
3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

10.1.3 Need for Both

There is a very important fact that is sometimes misunderstood:

The advent of asymmetric-key cryptography does not eliminate the need for symmetric-key cryptography.

Applications for Public-Key Cryptosystems

- **Encryption/decryption**
- **Digital signature**
- **Key exchange**

References

- **Chapter 10 -** Behrouz A Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, Mc Graw Hill, 3rd Edition, 2015.
- **Chapter 9 -** William Stallings, Cryptography and Network Security Principles and Practices, 7th Edition, Pearson Education, 2017.