UNIVERSITY OF RAJSHAHI

Rajshahi, BANGLADESH.

Course Code:

ICE-2241

Course Title :

Cryptography and Network security

Public key Cryptography and RSA

Key points of Public key cryptography

- Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys-
    - One a public key, and
    - One a private key.
- It is known as Public Key Encryption.
- Asymmetric encryption transforms plaintext into cipher-text using a one of the two keys and an encryption algorithm. Using the paired key and a decryption algorithm, the plaintext is recovered from the cipher-text.
- Asymmetric encryption can be used for ensuring…
    - **CONFIDENTIALITY** and
    - **Authentication** or **BOTH**.

Several common Misconception concerning Public-key encryption

- Public-key encryption is more secure from cryptanalysis than symmetric encryption.
- Public-key encryption is a general-purpose technique that has made symmetric encryption obsolete.
- Finally, there is a feeling that key distribution is insignificant when using public-key encryption, compared to the rather cumbersome handshaking involved with key distribution centers for symmetric encryption.

Public Key Cryptosystems

- Asymmetric algorithm rely on one key for encryption and a different but related key for decryption.

- **This algorithm have the following important characteristics:**
  - It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.
  - In addition, some algorithm (RSA) use either one of the two related keys for encryption, with the other used for decryption.

Asymmetric Encryption

A symmetric encryption has **SIX** ingredients:

✓Plaintext:

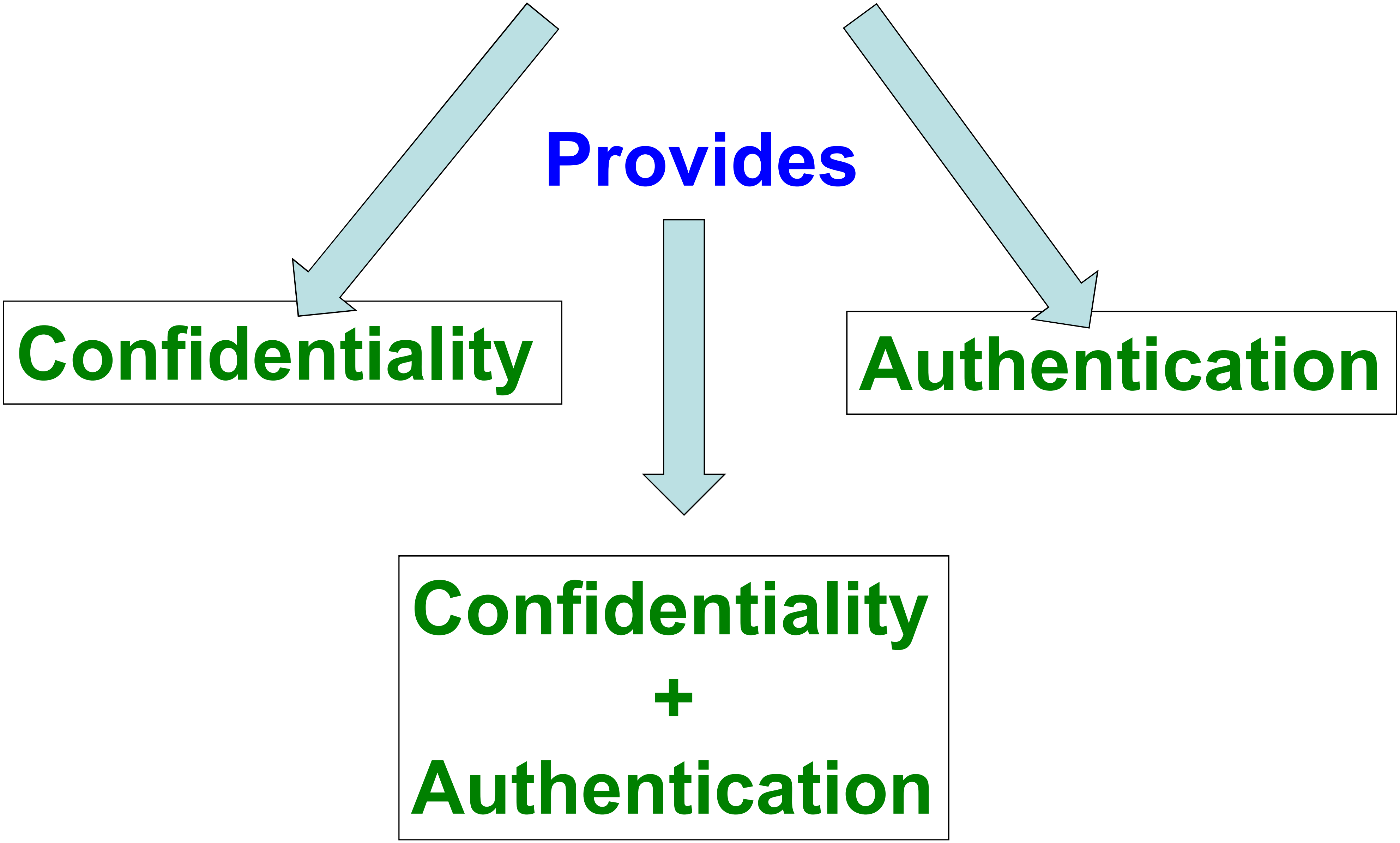
✓Encryption algorithm:

✓Public and Private key: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformation performed by the algorithm depends on the public or private key that is provided as input.

✓Ciphertext:

✓Decryption algorithm:

Public Key Encryption System



Provides

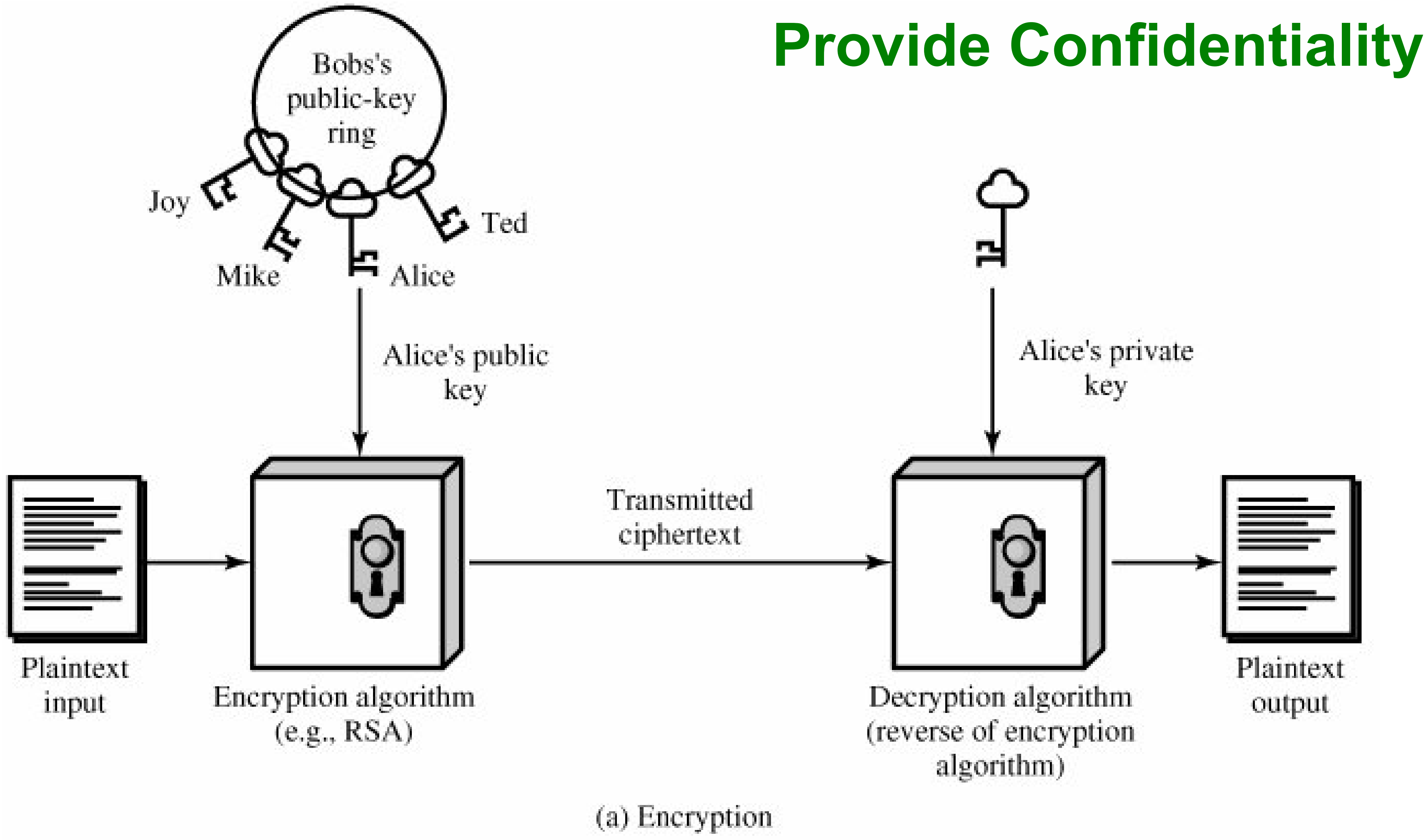
Confidentiality

Authentication

Confidentiality
+
Authentication

Public Key Encryption

Provide Confidentiality



(a) Encryption

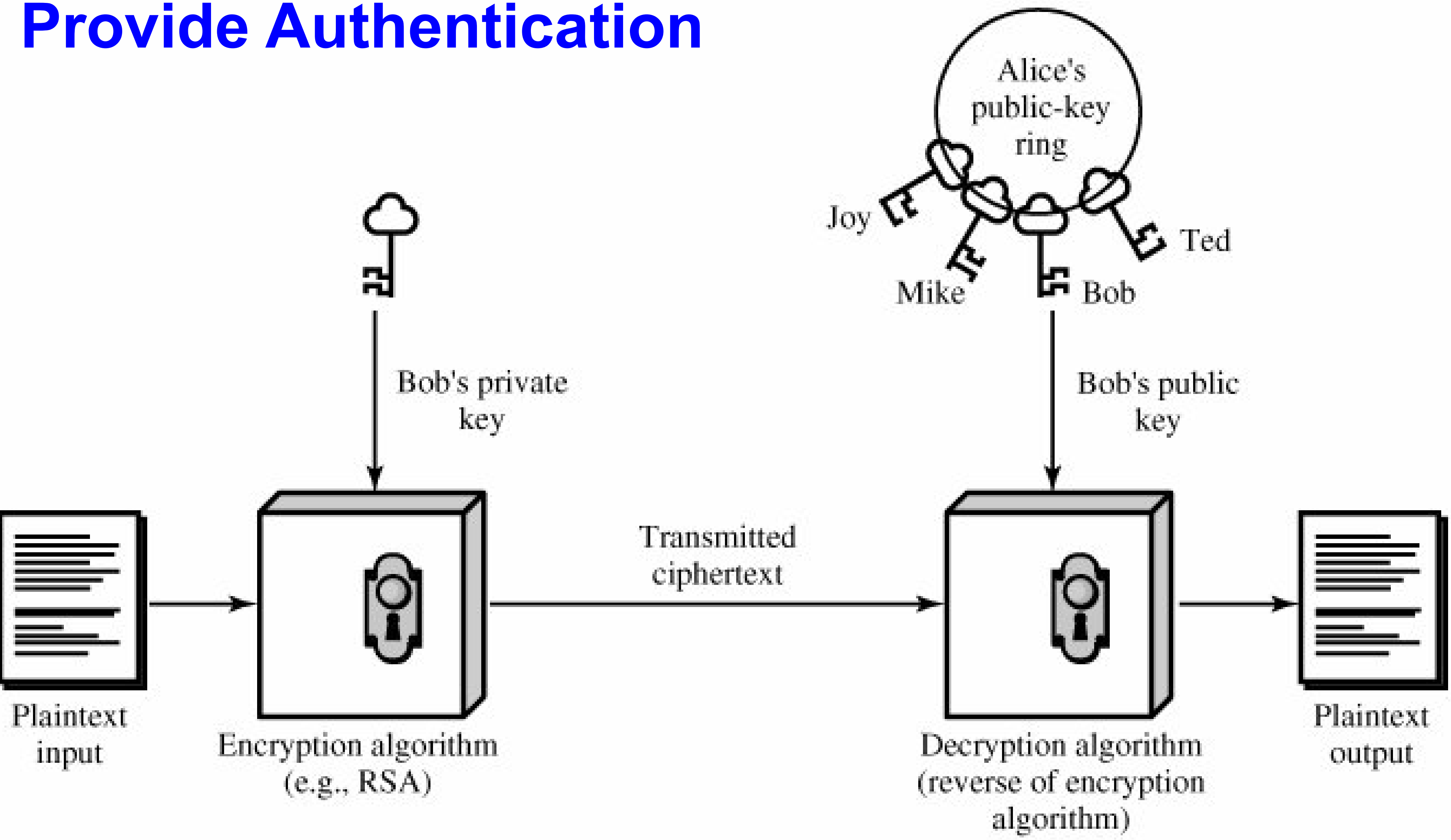
Then, Steps to Provide Confidentiality……

Public Key Encryption (Cont')

- With this approach, all participants have access to public keys, and private keys are generated locally by each participant and therefore need never be distributed.
- As long as a user's private key remains protected and secret, incoming communication is secure.
- At any time, a system can change its private key and publish the companion public key to replace its old public key.

Public Key Encryption

Provide Authentication



(b) Authentication

Then, Steps to Provide Authentication……

Digital Signature

- ✓ No one else has Bob’s private key and therefore no one else could have created a ciphertext that could be decrypted with Bob’s public key.
- ✓ Therefore, the entire encrypted message serves as a **DIGITAL SIGNATURE** .
- ✓it is impossible to alter the message without access to Bob’s private key, so the message is authenticated both in terms of source and in terms of data integrity.

Limitations of Digital Signature

?

- It is important to emphasize that the digital signature does not provide confidentiality.
- That is, the message being sent in safe from the alternation but not safe from eavesdropping.
- There is no protection of confidentiality because any observer can decrypt the message by using the sender’s public key.

Private Key Versus Public-Key Encryption

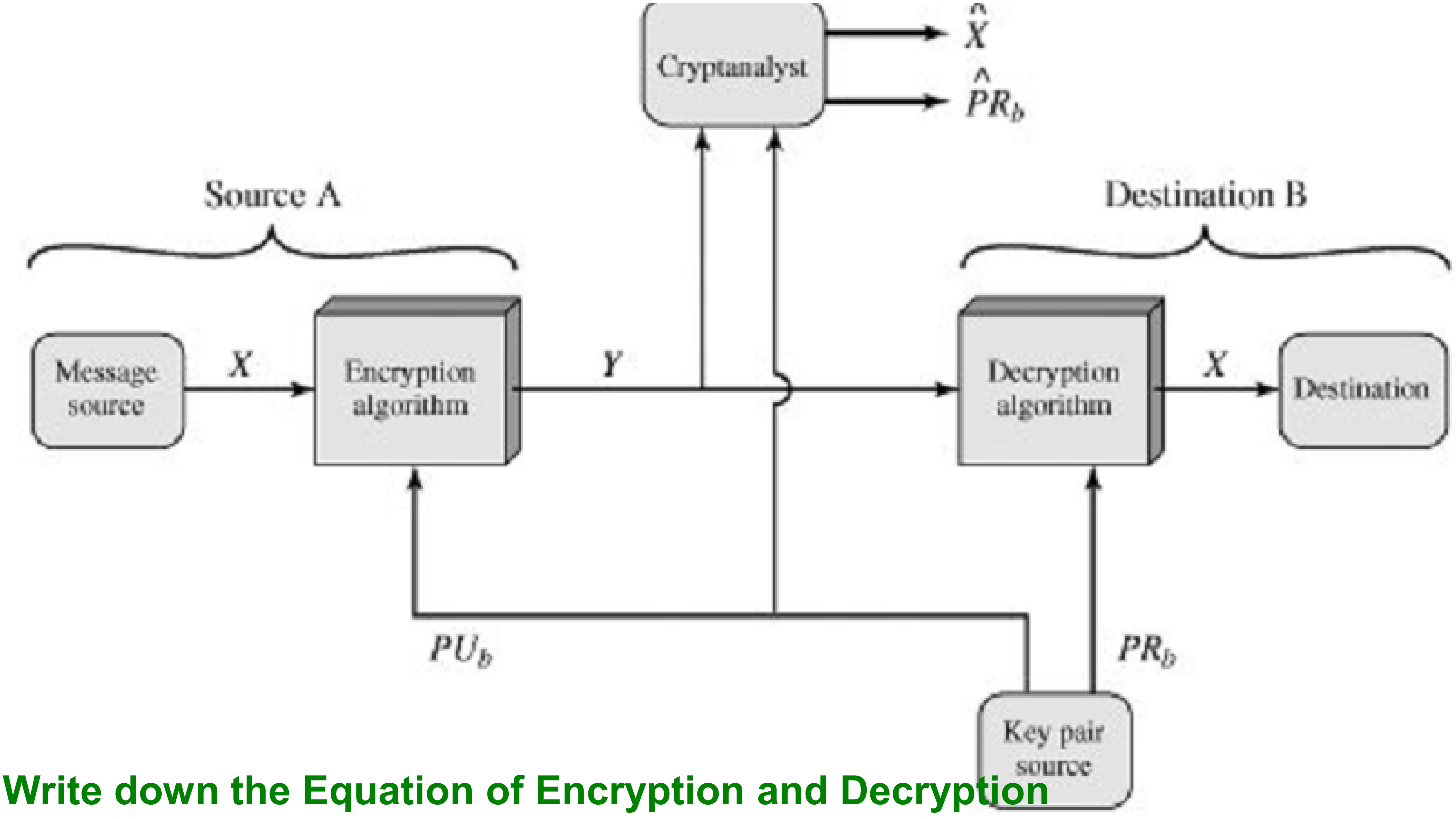
Private Key Encryption	Public Key Encryption
Needed to work: 1. The same algorithm with the same key is used for encryption and decryption.	**Needed to work:** 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
2. The sender and receiver must share the algorithm and the key.	2. The sender and receiver must each have one of the matched pair of keys (not the same one).
Needed for Security: 1. The key must be kept secret.	**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.	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.	3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Public Key Cryptosystem

Provide Confidentiality/Secrecy

$$Y= E\,(PU_b, X)$$

$$X= D(PR_b, Y)$$



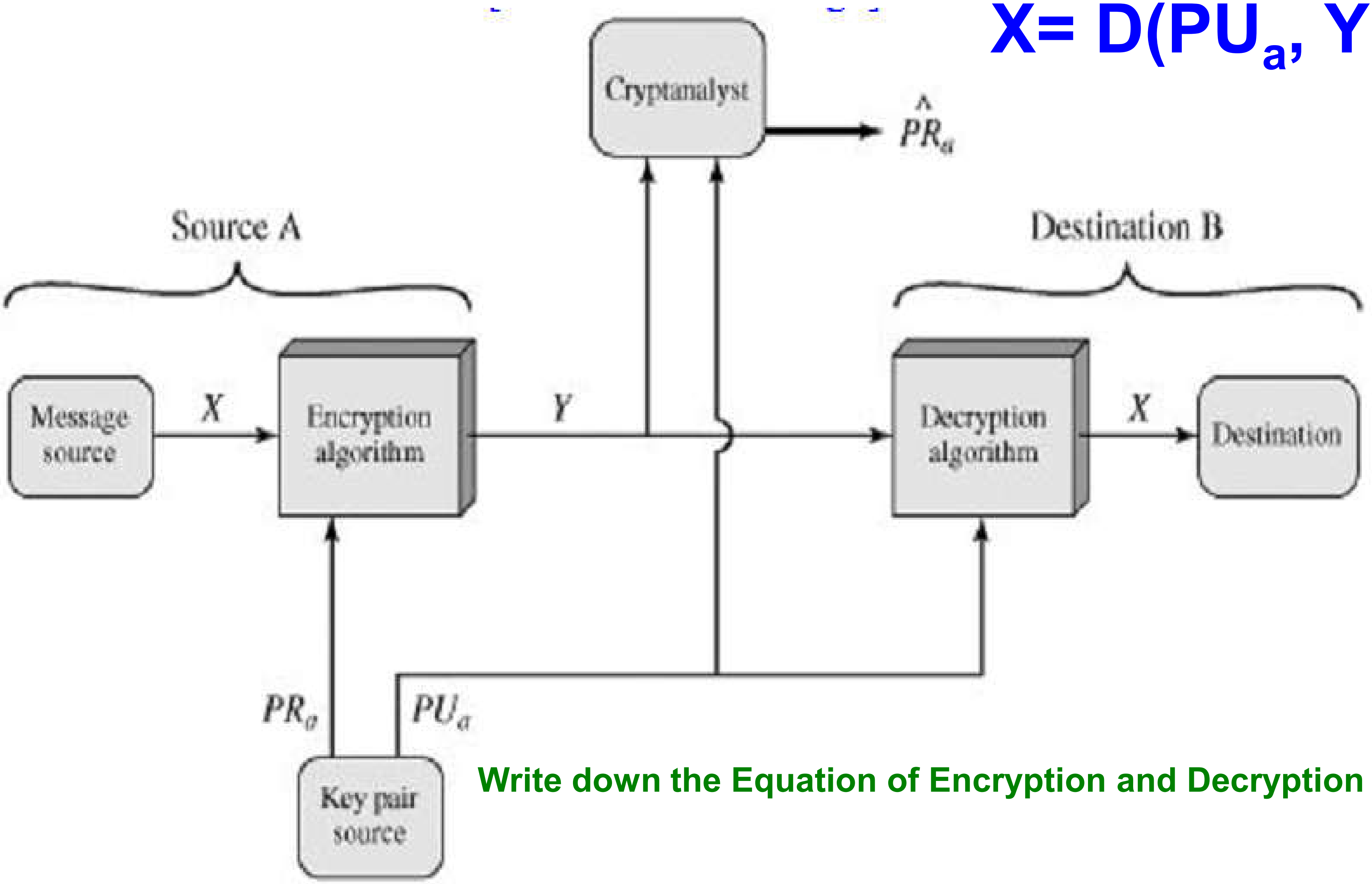
Write down the Equation of Encryption and Decryption

Public Key Cryptosystem

Provide Authentication

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

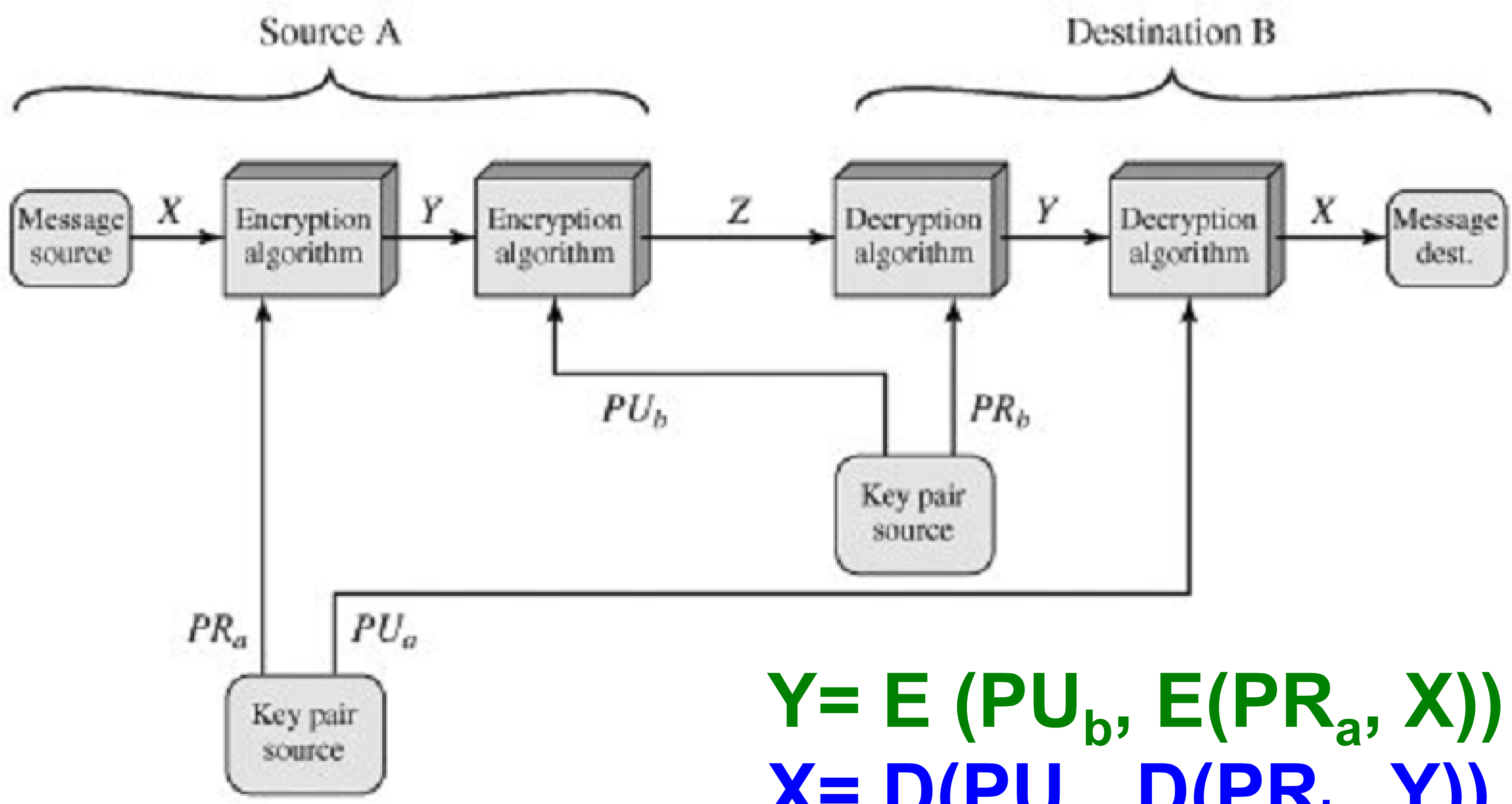
$$X = D(PU_a, Y)$$



Write down the Equation of Encryption and Decryption

Public Key Cryptosystem

Provide Authentication and Confidentiality



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

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

Write down the Equation of Encryption and Decryption

Applications for Public-Key Cryptosystems

In broad terms, we can classify the use of public-key cryptosystems into <u>**THREE**</u> categories:

✓**Encryption/decryption:** The sender encrypts a message with the recipient's public key.

✓**Digital signature:** The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

✓ **Key exchange:** Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

Requirements for Public-Key Cryptography

- ✓ It is computationally easy for a party B to generate a pair (public key PU_b, private key PR_b).
- ✓ It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext:

$$C = E(PU_b, M)$$

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

$$M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$$

Requirements for Public-Key Cryptography (Con’t)

- ✓ It is computationally infeasible for an adversary, knowing the public key, **PU_b**, to determine the private key, **PR_b**.
- ✓ It is computationally infeasible for an adversary, knowing the public key, **PU_b**, and a ciphertext, C, to recover the original message, M.
- ✓ We can add a sixth requirement that, although useful, is not necessary for all public-key applications:
- ✓ The two keys can be applied in either order:

$$M = D[PU_b, E(PR_b, M)] = D[PR_b, E(PU_b, M)]$$

One Way Hash Function

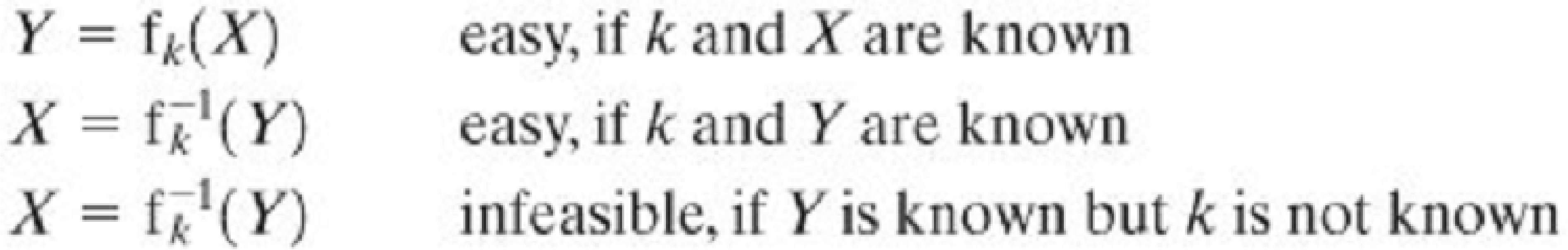
A ***one-way function*** is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy whereas the calculation of the inverse is infeasible.

$Y = f(X)$ **easy**

$X = f^{-1}(X)$ **infeasible**

Trap-door one-way function

- It is a function which is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known.
- With the additional information the inverse can be calculated in polynomial time.
- We can summarize as follows: A trap-door one-way function is a family of invertible functions f_k, such that



$Y = f_k(X)$	easy, if k and X are known
$X = f_k^{-1}(Y)$	easy, if k and Y are known
$X = f_k^{-1}(Y)$	infeasible, if Y is known but k is not known

The RSA Algorithm

The scheme developed by Rivest, Shamir, and Adleman makes use of an expression with exponentials. Plaintext is encrypted in blocks.

The RSA scheme is a block cipher(**?**) in which the plaintext and ciphertext are integers between 0 and n 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024}.

For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:

✓ It is possible to find values of e, d, n such that M^{ed} mod n = M for all M < n.

✓ It is relatively easy to calculate M^e mod n and C^d mod n for all values of M < n.

✓ It is infeasible to determine d given e and n.

The RSA Algorithm

The scheme developed by Rivest, Shamir, and Adleman makes use of an expression with exponentials. Plaintext is encrypted in blocks.

The RSA scheme is a block cipher(**?**) in which the plaintext and ciphertext are integers between 0 and n 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024}.

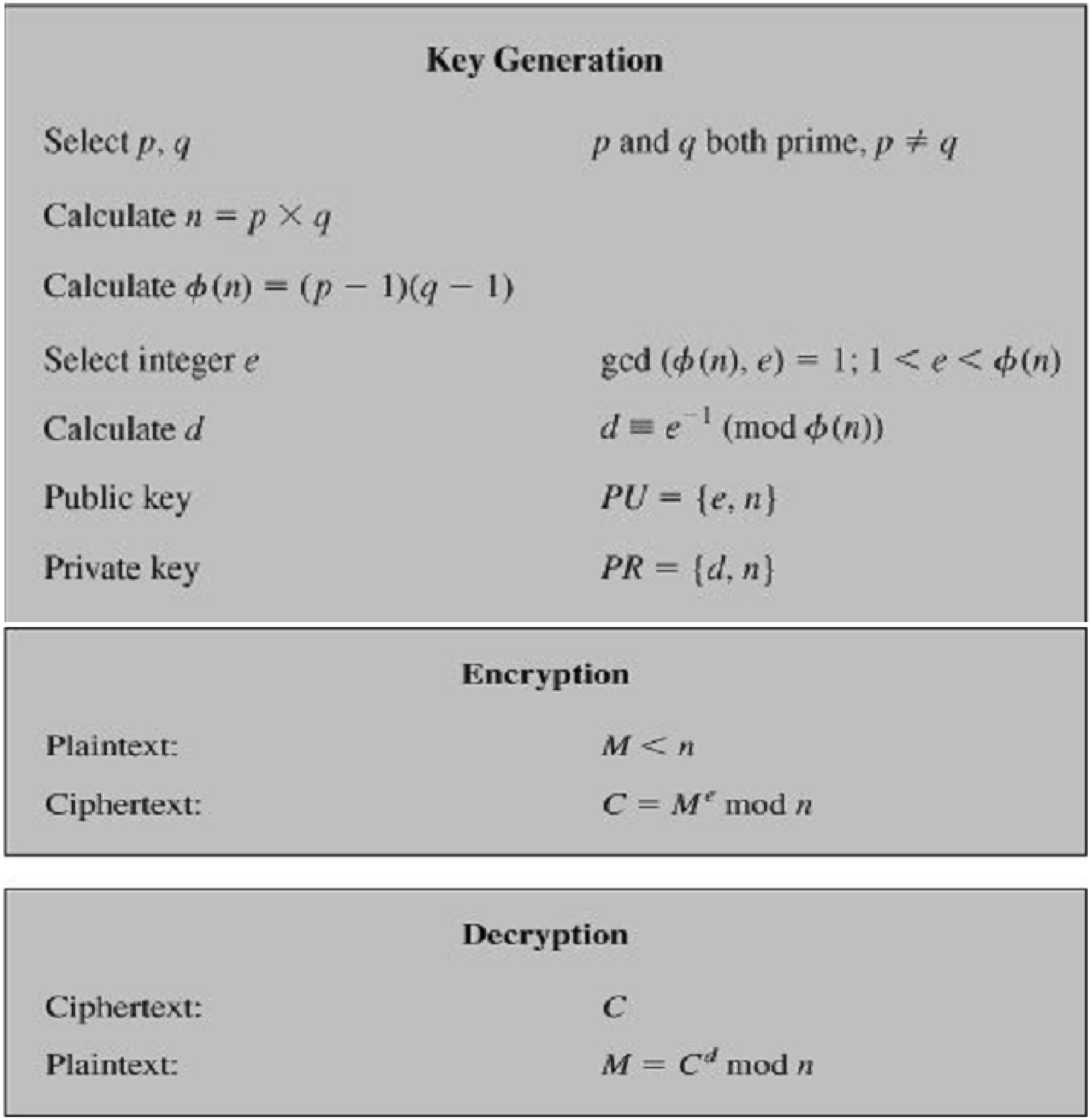
For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:

✓ It is possible to find values of e, d, n such that M^{ed} mod n = M for all M < n.

✓ It is relatively easy to calculate mod M^e mod n and C^d for all values of M < n.

✓ It is infeasible to determine d given e and n.

The RSA Algorithm (Cont’)



Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

The Security of RSA

Four possible approaches to attacking the RSA algorithm are as follows:

Brute force: This involves trying all possible private keys.

Mathematical attacks: There are several approaches, all equivalent in effort to factoring the product of two primes.

Timing attacks: These depend on the running time of the decryption algorithm.

Chosen ciphertext attacks: This type of attack exploits properties of the RSA algorithm.

The defense against the brute-force approach is the same for RSA as for other cryptosystems, namely, use a large key space. Thus, the larger the number of bits in d, the better. However, because the calculations involved, both in key generation and in encryption/decryption, are complex, the larger the size of the key, the slower the system will run.