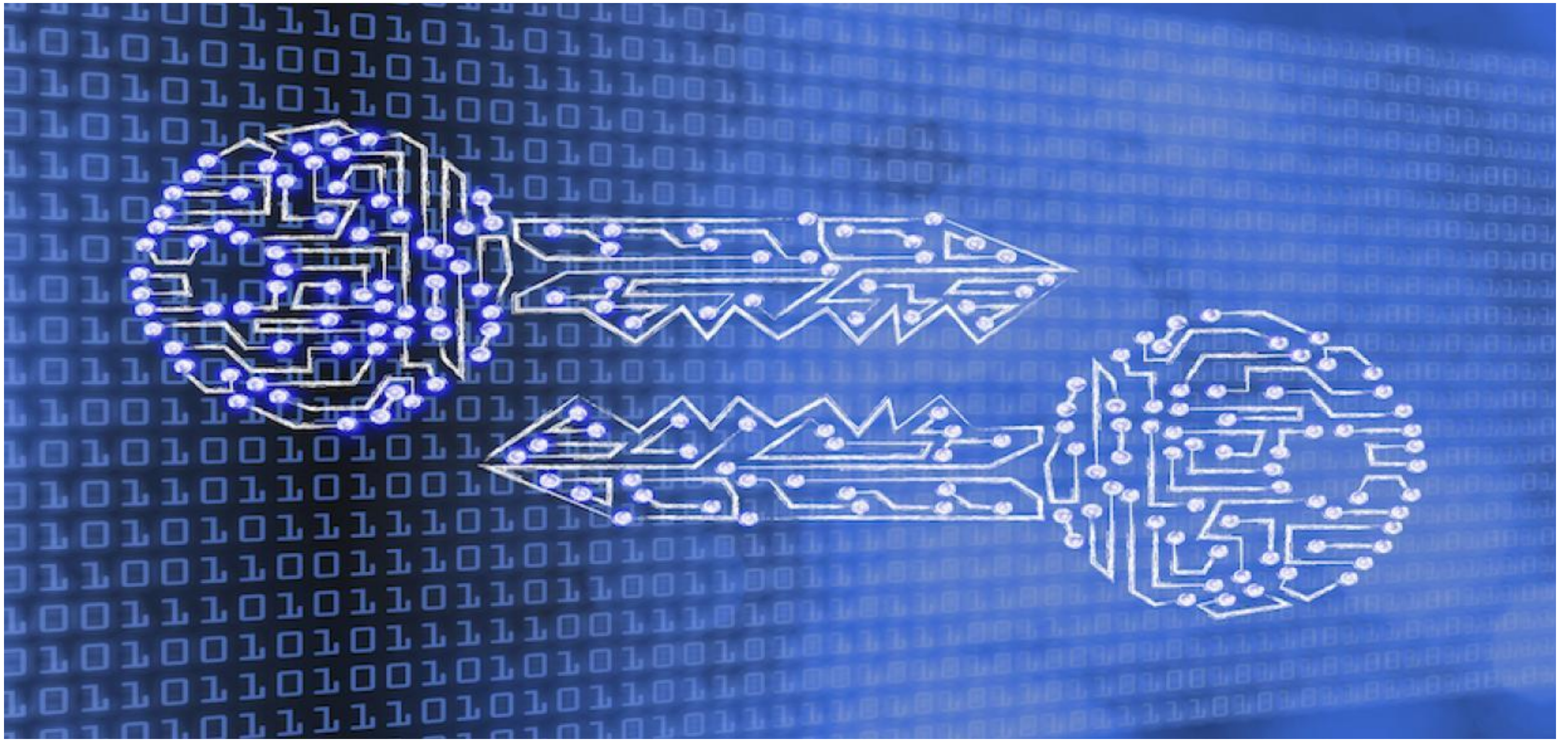
Chapter 31

Cryptography And Network Security



Objective

- Confidentiality, integrity, and availability

  - confidentiality is threatened by attacks such as snooping and traffic analysis.

  - how integrity is threatened by attacks such as modification, masquerading, replaying, and repudiation.

  - one attack that threatens availability, denial of service.

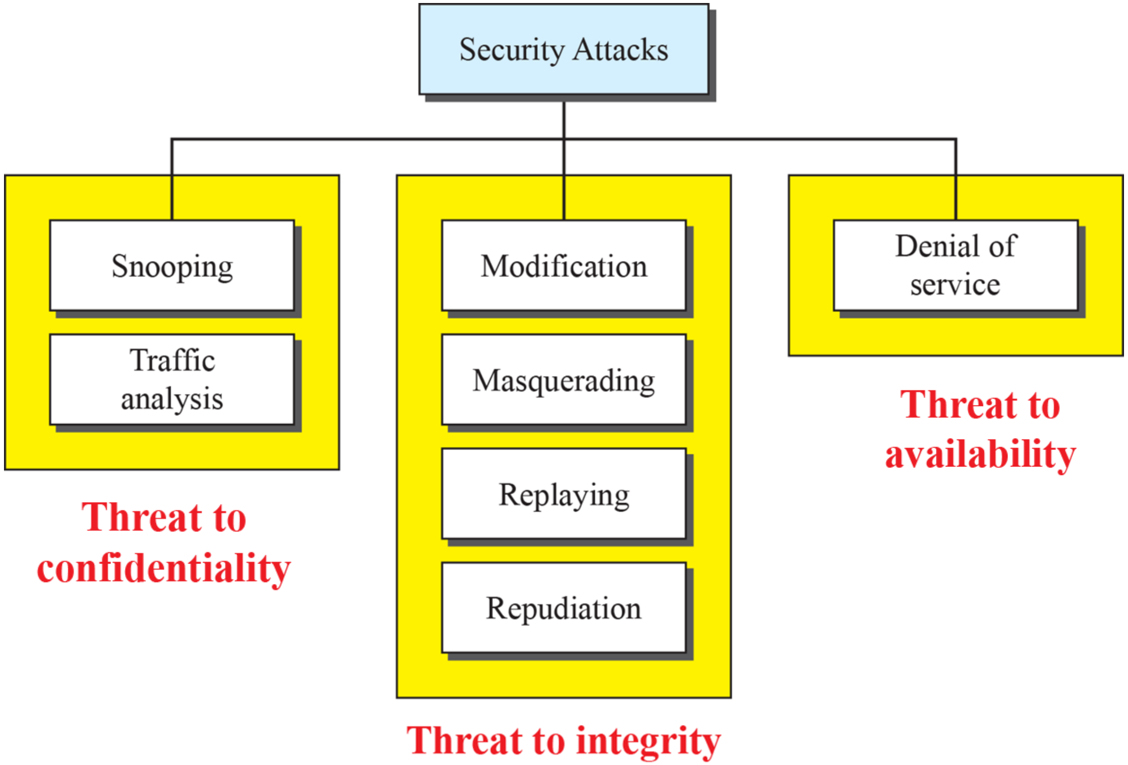
- Cryptography and Steganography

Introduction

- Let us first discuss three security goals: confidentiality, integrity, and availability.
- To be secured, information needs to be hidden from unauthorized access – confidentiality.
- Protected from unauthorized change – integrity.
- Available to an authorized entity when it is needed - availability.

Attacks

- Our three goals of security, confidentiality, integrity, and availability, can be threatened by security attacks.



Taxonomy of attacks with relation to security goals

Services and Techniques

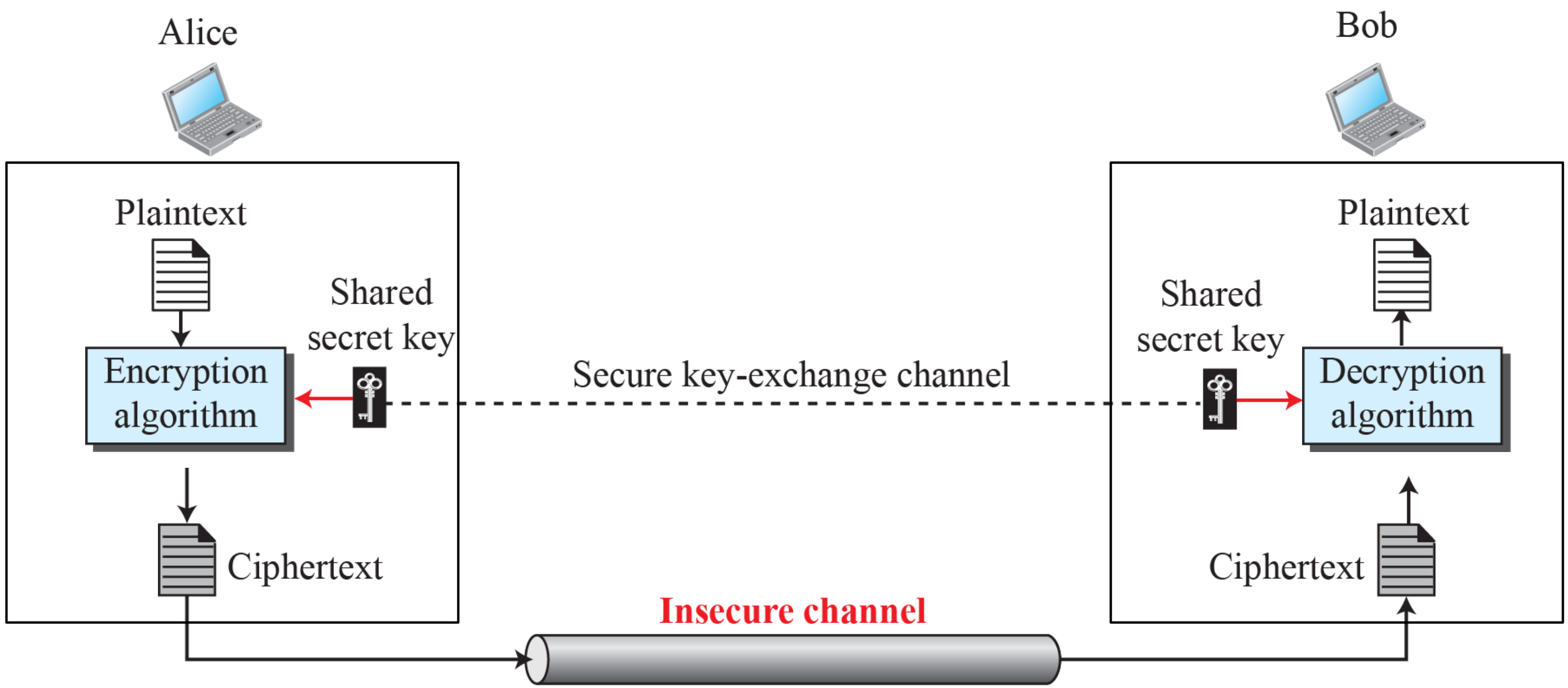
- ITU-T defines some security services to achieve security goals and prevent attacks.

- Two techniques are prevalent today: one is very general (cryptography) and one is specific (steganography).

Confidentiality

- Confidentiality can be achieved using ciphers.
- Ciphers can be divided into two broad categories: symmetric-key and asymmetric-key.
- A symmetric-key cipher uses the same key for both encryption and decryption, and the key can be used for bidirectional communication, which is why it is called symmetric.

Symmetric-Key Ciphers



Symmetric-key encipherment as locking and unlocking with the same key

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 →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Representation of plaintext and ciphertext characters inmodulo 26

Example

- Use the additive cipher with key = 15 to encrypt the message "hello".

Solution

We apply the encryption algorithm to the plaintext, character by character:

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

The result is "WTAAD". Note that the cipher is monoalphabetic because two instances of the same plaintext character (*l*) are encrypted as the same character (*A*).

Example

- Use the additive cipher with key = 15 to decrypt the message "WTAAD".

Solution

We apply the decryption algorithm to the plaintext character by character:

Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

The result is "hello". Note that the operation is in modulo 26, which means that we need to add 26 to a negative result (for example −15 becomes 11).

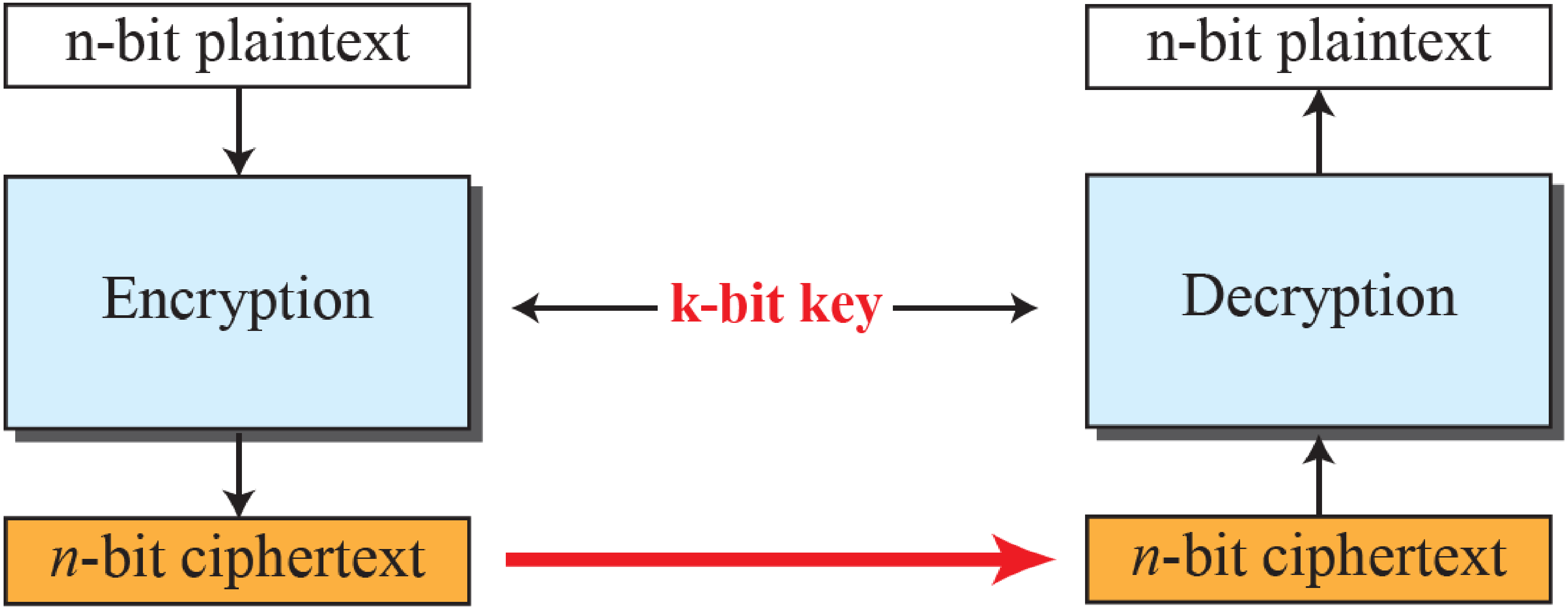
Example

An example key for a monoalphabetic substitution cipher

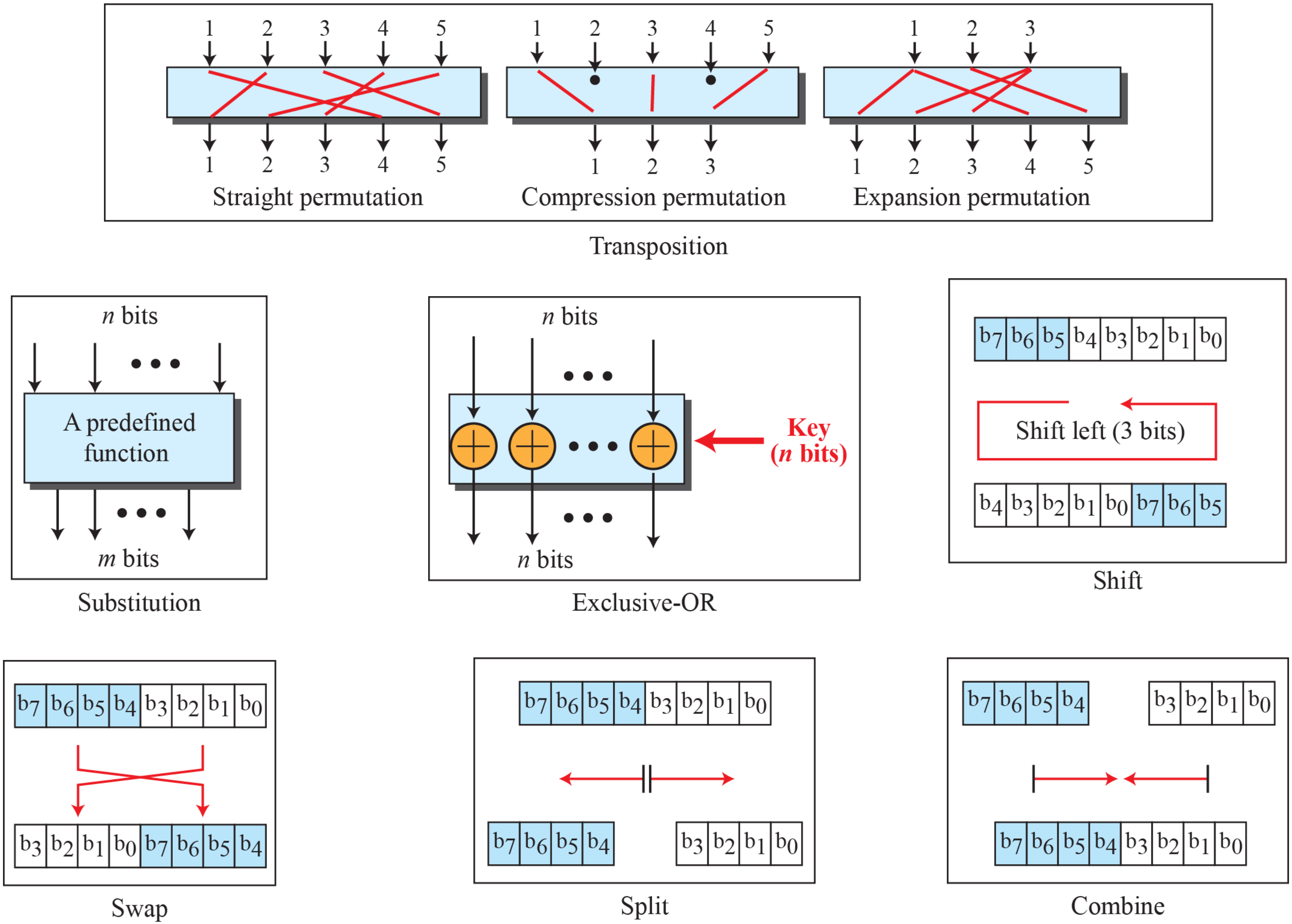
Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	N	O	A	T	R	B	E	C	F	U	X	D	Q	G	Y	L	K	H	V	I	J	M	P	Z	S	W

- We can use the key in to encrypt the message

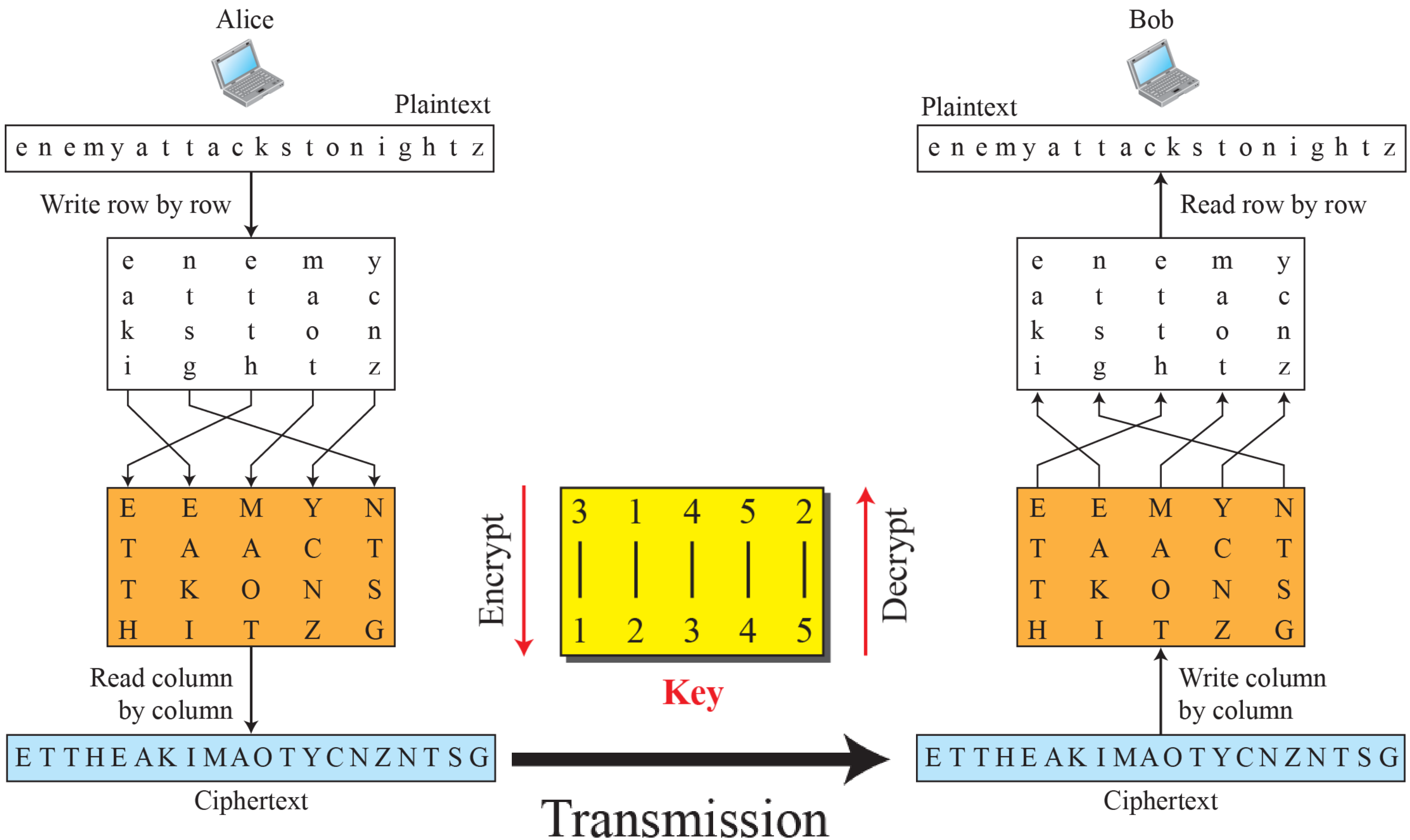
Plaintext:	this message is easy to encrypt but hard to find the key
Ciphertext:	ICFVQRVVNERFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS



A modern block cipher



Components of a modern block cipher

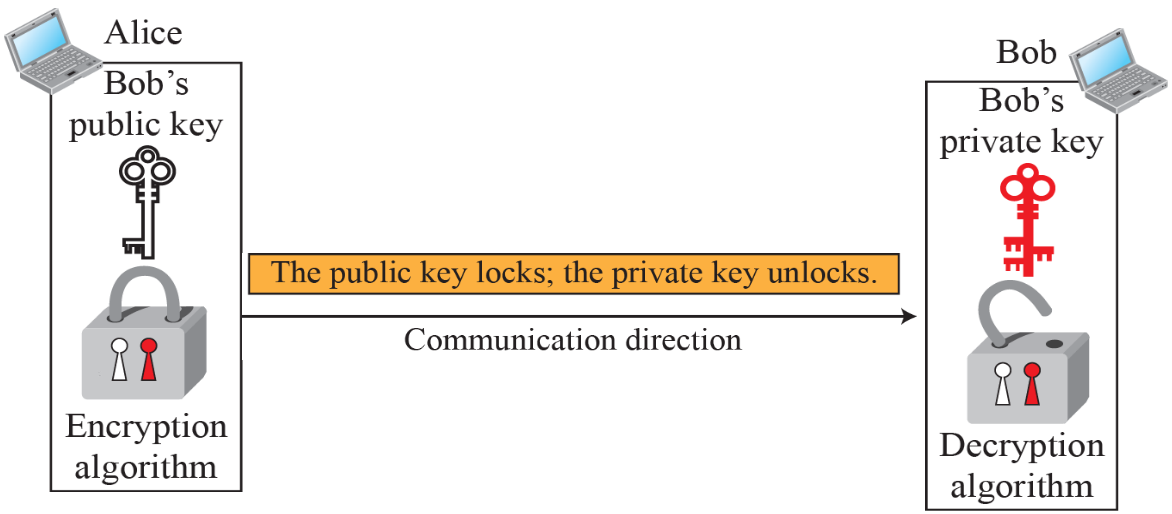


Transposition cipher

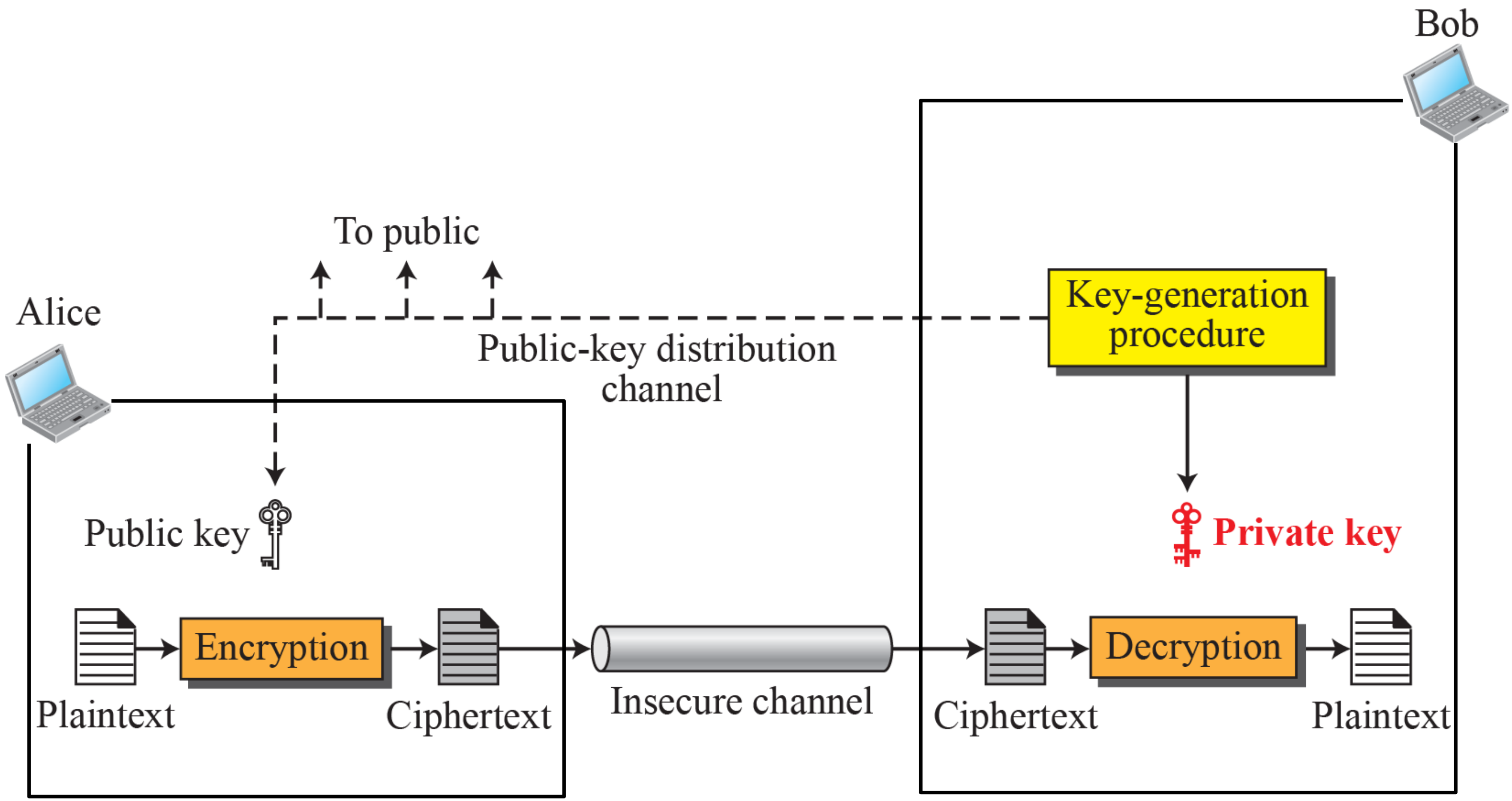
Asymmetric-Key Ciphers

- Symmetric- and asymmetric-key ciphers will exist in parallel and continue to serve the community.

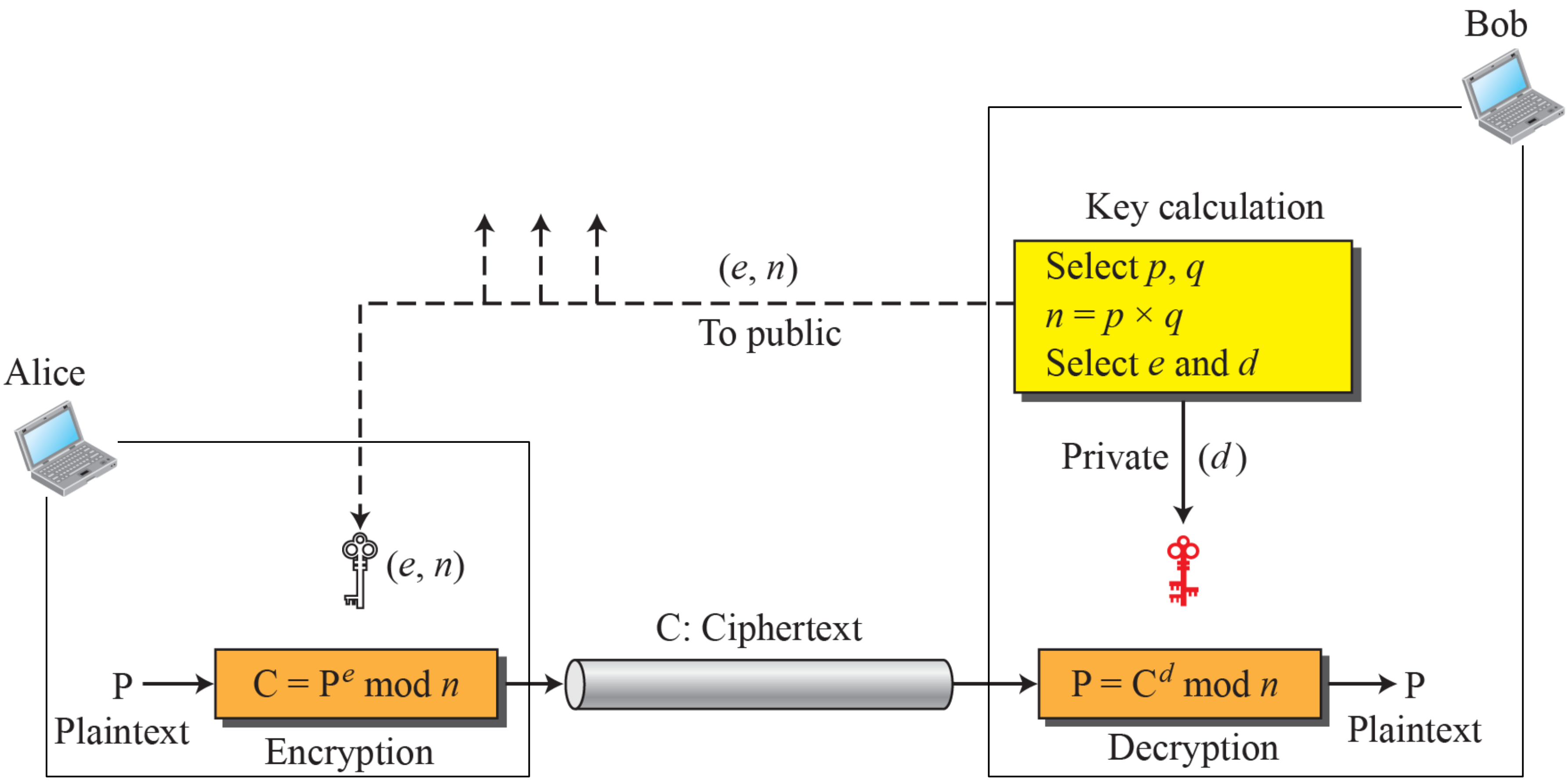
- We actually believe that they are complements of each other; the advantages of one can compensate for the disadvantages of the other.



Locking and unlocking in asymmetric-key cryptosystem



General idea of asymmetric-key cryptosystem



Encryption, decryption, and key generation in RSA

Example

- Let Bob choose 7 and 11 as p and q and calculate $n = 7 \times 11 = 77$, $\phi(n) = (7 - 1)(11 - 1)$, or 60.
- If he chooses e to be 13, then d is 37. Note that $e \times d \bmod 60 = 31$. Now imagine that Alice wants to send the plaintext 5 to Bob.
- She uses the public exponent 13 to encrypt 5. This system is not safe because p and q are small.

Plaintext: 5		Ciphertext: 26
$C = 5^{13} = 26 \bmod 77$		$P = 26^{37} = 5 \bmod 77$
Ciphertext: 26		Plaintext: 5

Realistic Example

- We choose a 512-bit p and q, calculate n and ϕ(n).
- We then choose e and calculate d. Finally, we show the results of encryption and decryption. The integer p is a 159-digit number.

p =	96130345313583504574191581280615427909309845594996215822583150879647940455056470638491257160180347503120986666064924201918087806674210960633542199266612 09

Example(continued)

The integer q is a 160-digit number.

q =	12060191957231446918276794204450896001555925054637033936061798321731482148483764659215389453209175225273226830107120695604602513887145524969000359660045617

The modulus $n = p \times q$. It has 309 digits.

n =	115935041739676149688925098646158875237714573754541447754855261376147885408326350817276878815968325168468849300625485764111250162414552339182927162507656772727460097082714127730434960500556347274566628060099924037102991424472292215772798531727033839381334692684137327622000966676671831831088373420823444370953

$\phi(n) = (p - 1)(q - 1)$ has 309 digits.

$\phi(n)$ =	115935041739676149688925098646158875237714573754541447754855261376147885408326350817276878815968325168468849300625485764111250162414552339182927162507656751054233608492916752034482627988117554787657013923444405716989581728196098226361075467211864612171359107358640614008885170265377277264467341066243857664128

Example(continued)

Bob chooses e = 35535 (the ideal is 65537). He then finds d.

e =	35535
d =	5800830286003776393609366128967791759466906208965096218042286611138059385282235873170628691003002171085904433840217072986908760061153062025249598844480475682409662470814858171304632406440777048331340108509473852956450719367740611973265574242372176176746207763716420760033708533328853214470885955136670294831

Alice wants to send the message “THIS IS A TEST”, which can be changed to a numeric value using the 00–26 encoding scheme (26 is the *space* character).

P =	1907081826081826002619041819

Example(continued)

The ciphertext calculated by Alice is $C = P^e$, which is shown below.

C =	4753091236462268272063655506105451809423717960704917165232392430544 5296061319932856661784341835911415119741125200568297979457173603610 1278218847892741566090480023507190715277185914975188465888632101148 3541033616578984679683867637337657774656250792805211481418440481418 443081277305900469287424855916646210865 6

Bob can recover the plaintext from the ciphertext using $P = C^d$, which is shown below.

P =	1907081826081826002619041819

The recovered plaintext is "THIS IS A TEST" after decoding.

Other Aspects of Security

- The cryptography systems that we have studied so far provide confidentiality.
- However, in modern communication, we need to take care of other aspects of security, such as integrity, message and entity authentication, nonrepudiation, and key management.

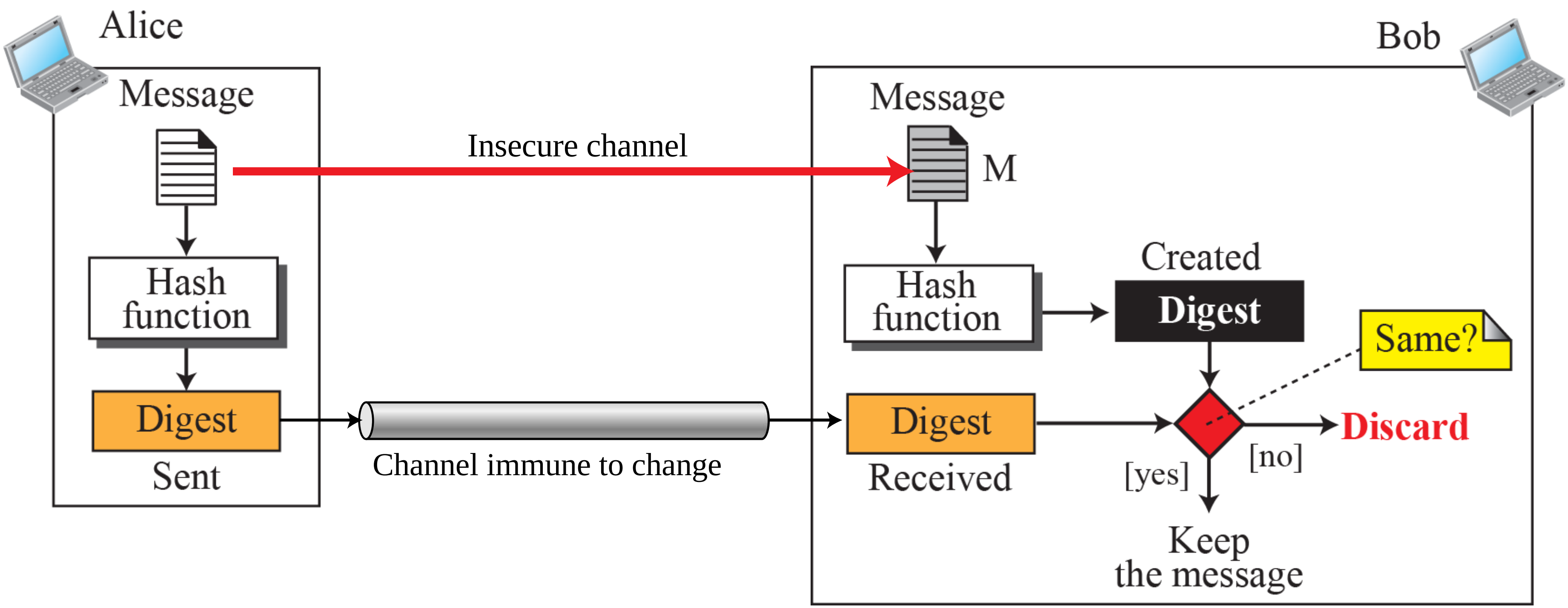
Message Integrity

- There are occasions where we may not even need secrecy but instead must have integrity: the message should remain unchanged.

- For example, Alice may write a will to distribute her estate upon her death. The will does not need to be encrypted. After her death, anyone can examine the will.

- The integrity of the will, however, needs to be preserved. Alice does not want the contents of the will to be changed.

Message digest

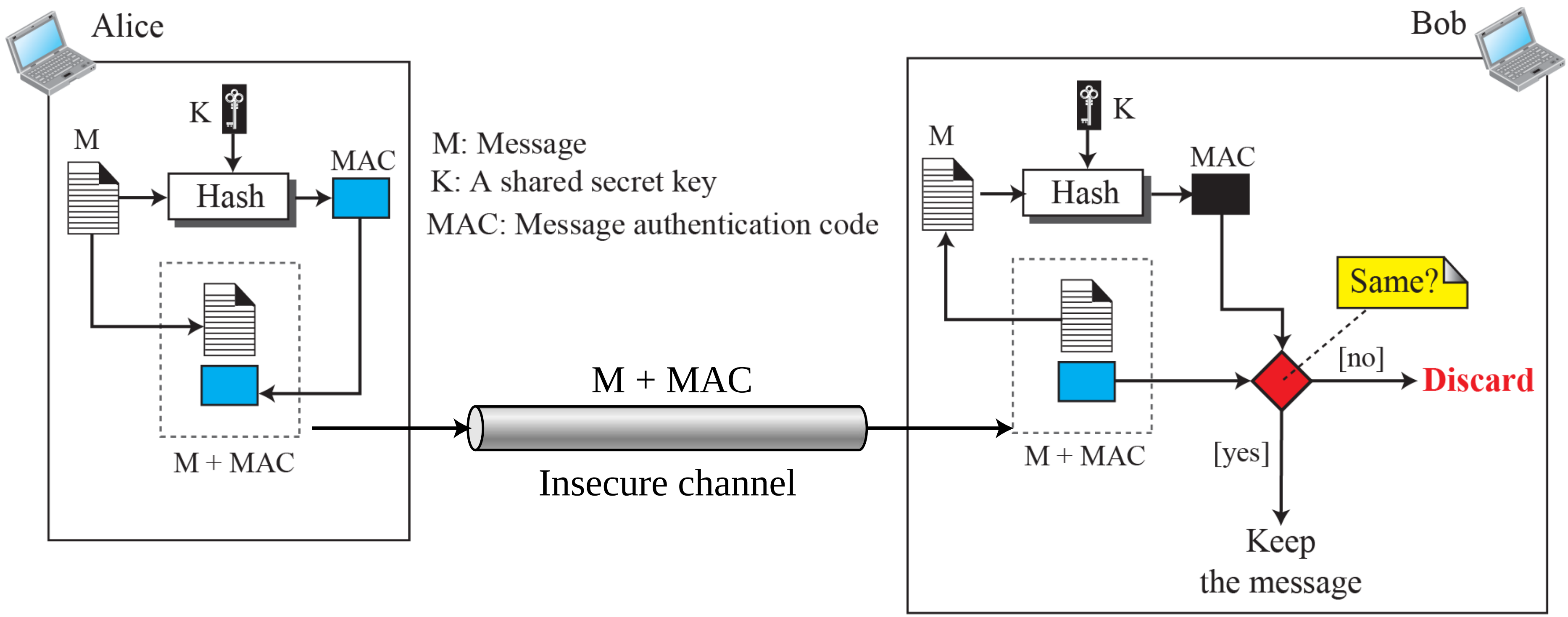


Message and digest

Message Authentication

- A digest can be used to check the integrity of a message - that the message has not been changed.
- To ensure the integrity of the message and the data origin authentication - that Alice, not somebody else, is the originator of the message - we need to include a secret shared by Alice and Bob (that Eve does not possess) in the process.
- We need to create a message authentication code (MAC).

MAC

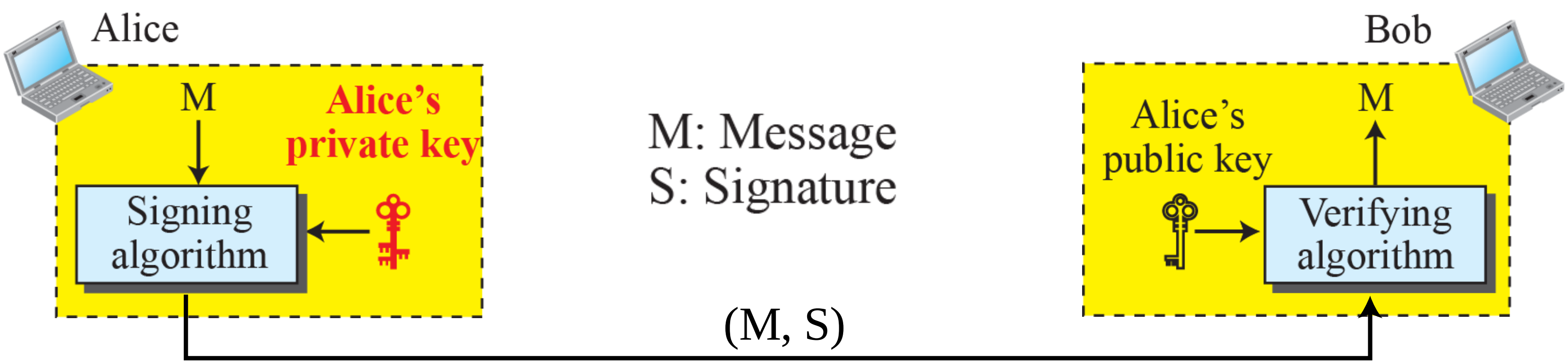


Message authentication code

Digital Signature

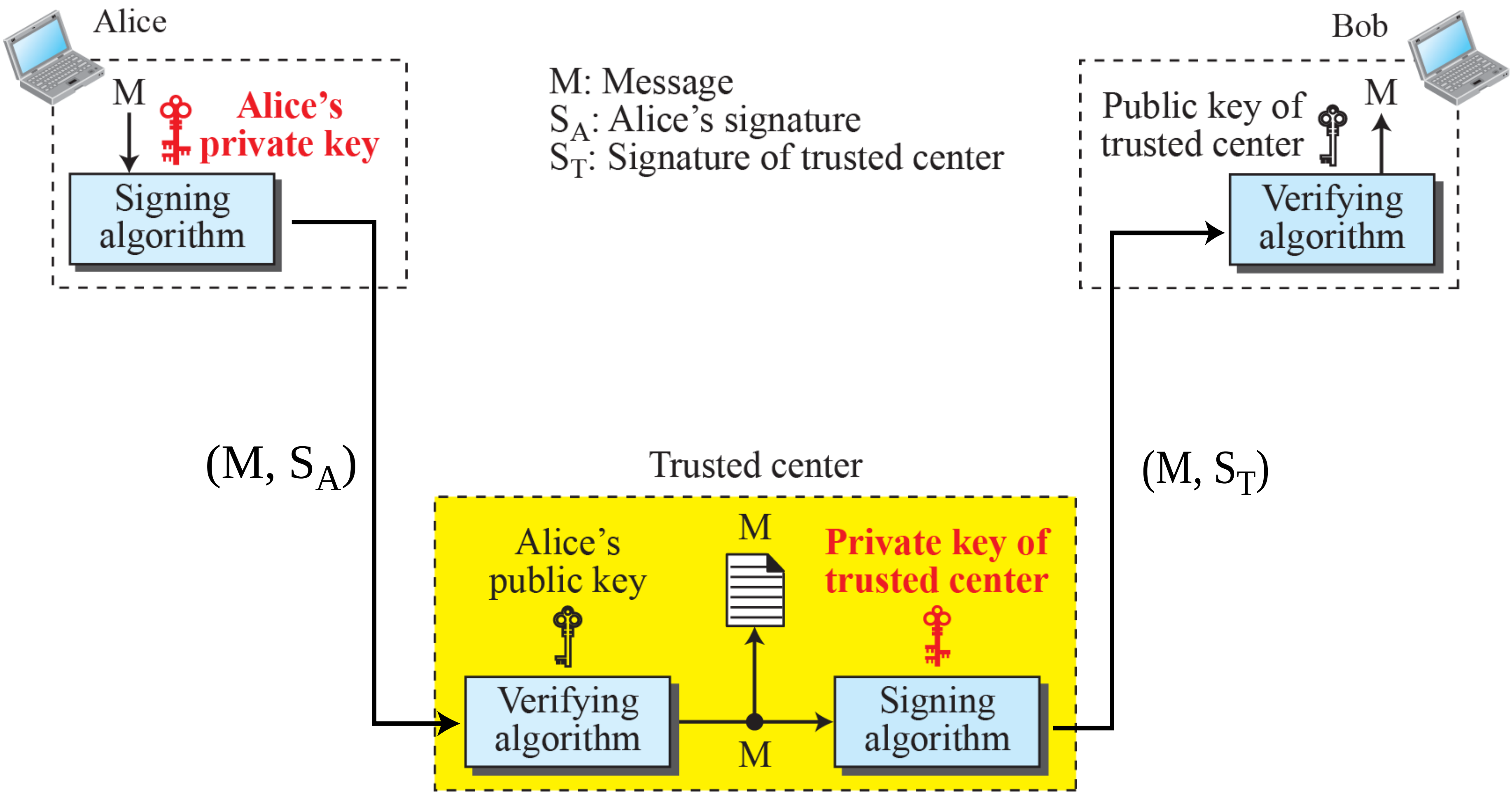
- Another way to provide message integrity and message authentication is a digital signature.

- A MAC uses a secret key to protect the digest; a digital signature uses a pair of private-public keys.

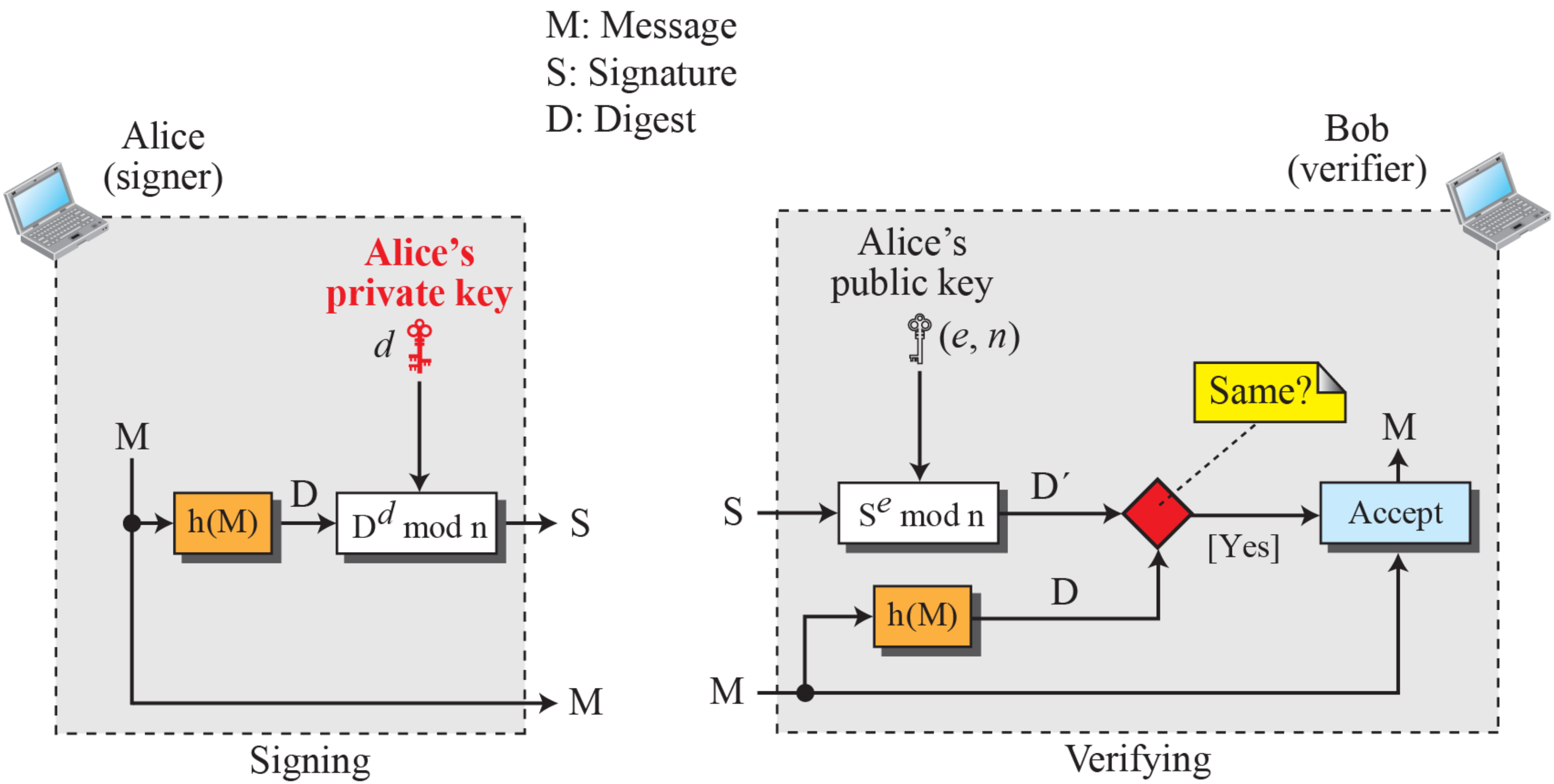


Digital signature process

Non-repudiation



Using a trusted center for non-repudiation



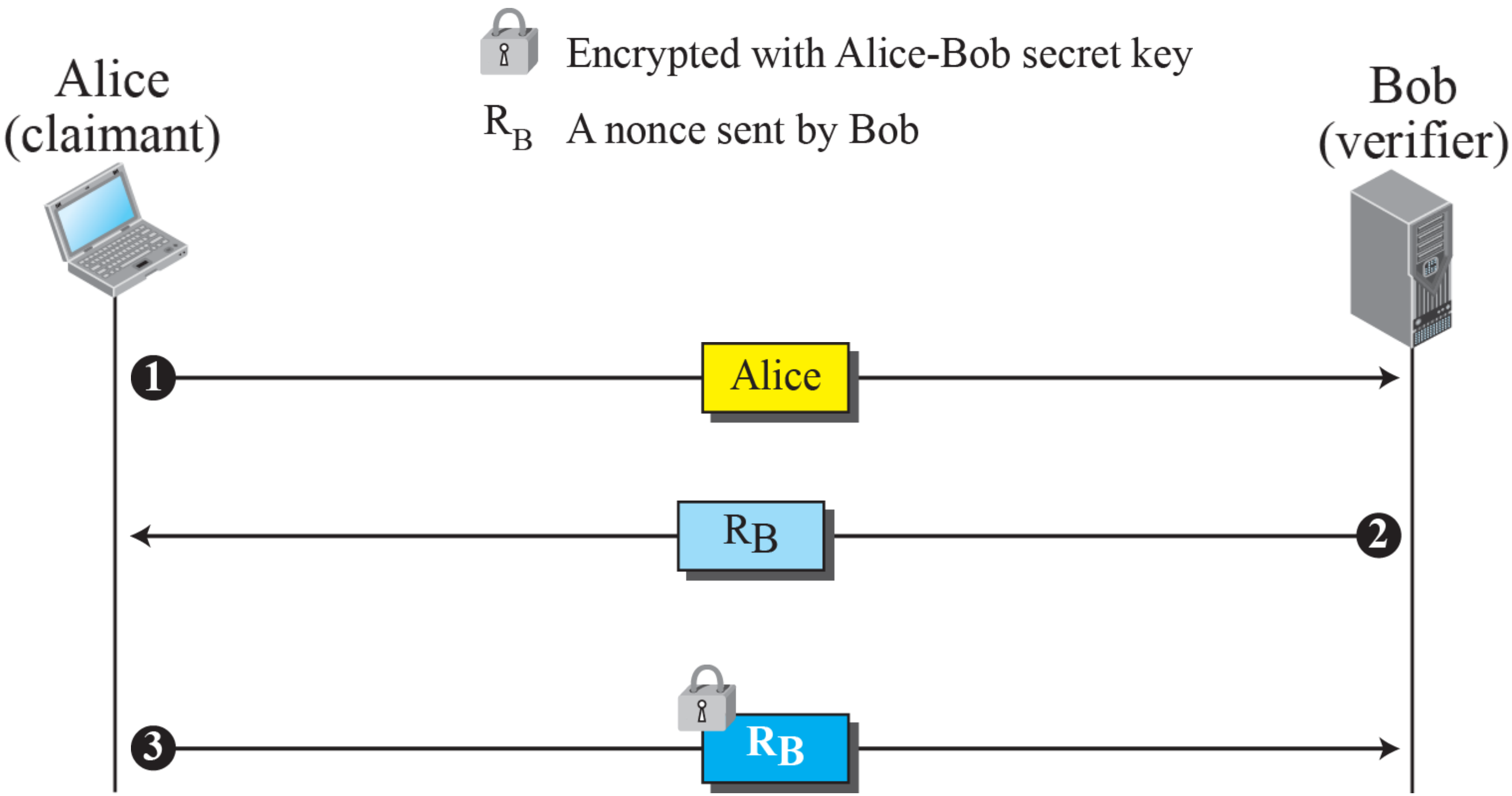
The RSA signature on the message digest

Entity Authentication

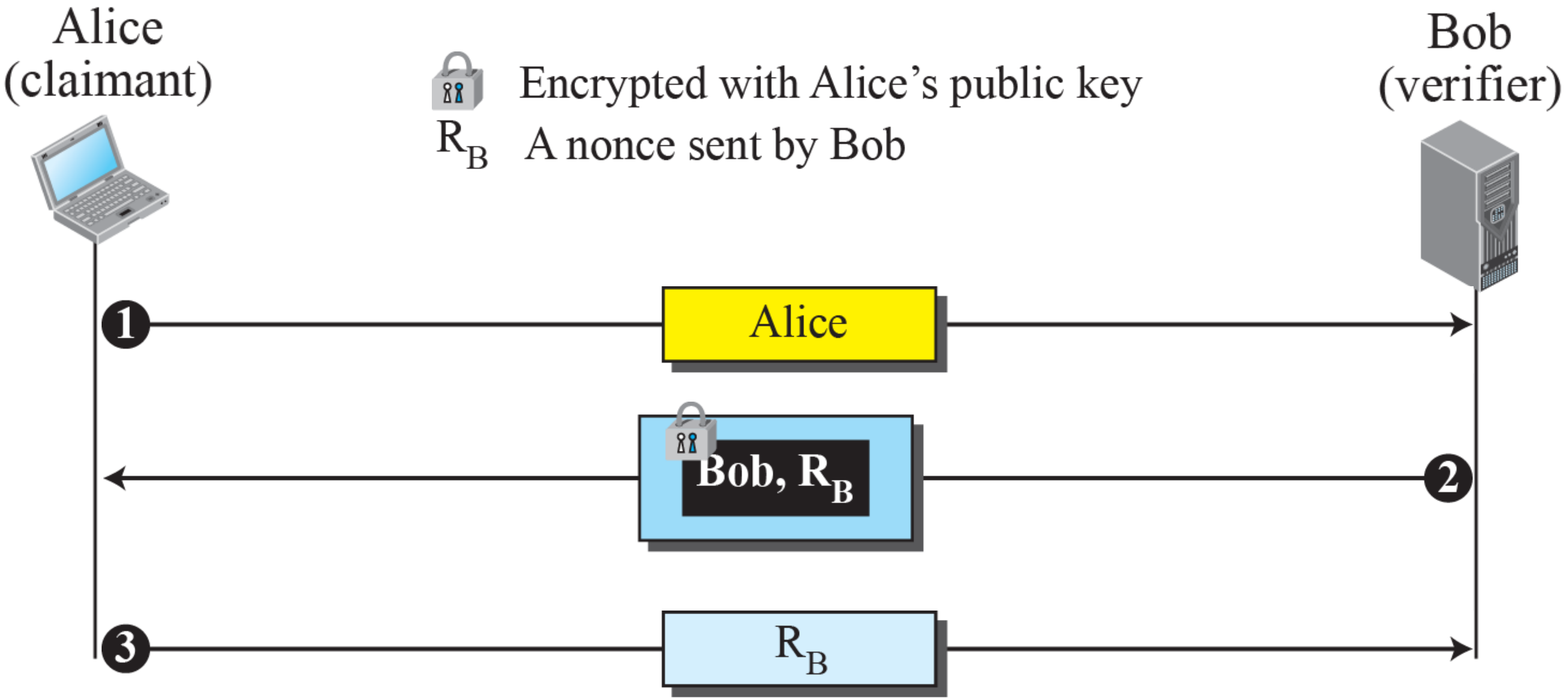
- Entity authentication is a technique designed to let one party verify the identity of another party.

- An entity can be a person, a process, a client, or a server.

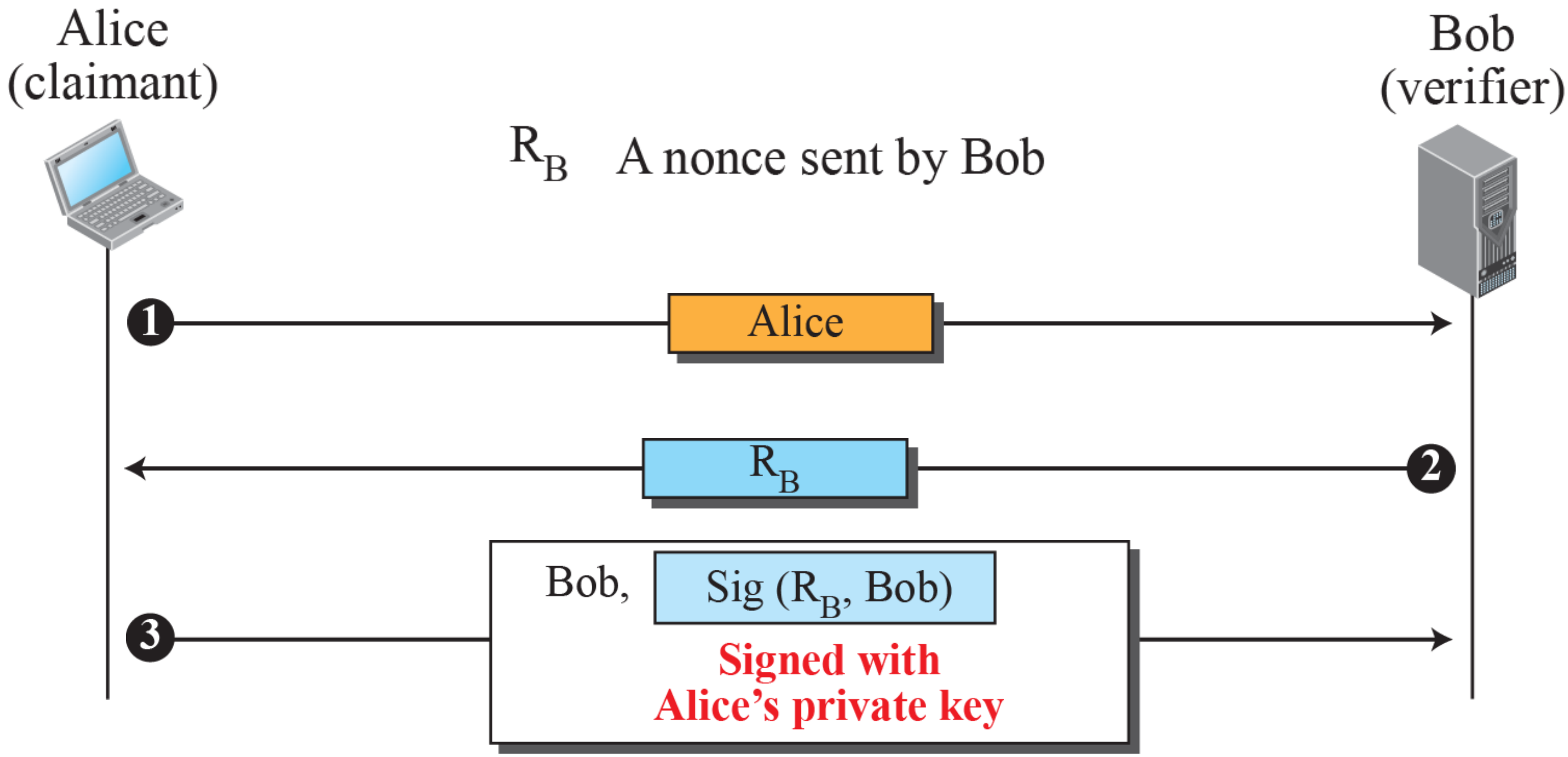
- The entity whose identity needs to be proven is called the claimant; the party that tries to verify the identity of the claimant is called the verifier.



Unidirectional, symmetric-key authentication



Unidirectional, asymmetric-key authentication

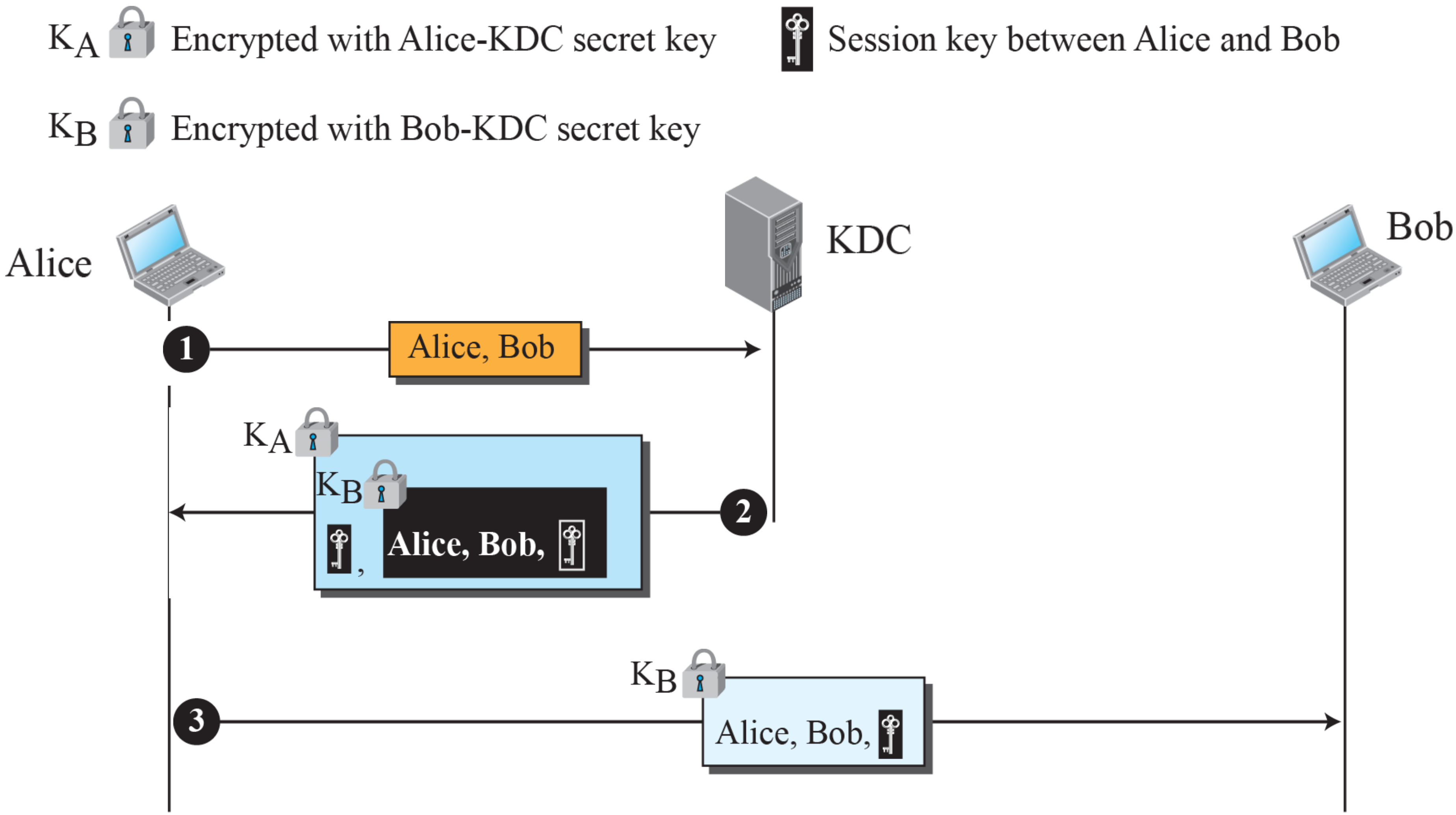


Digital signature, unidirectional authentication

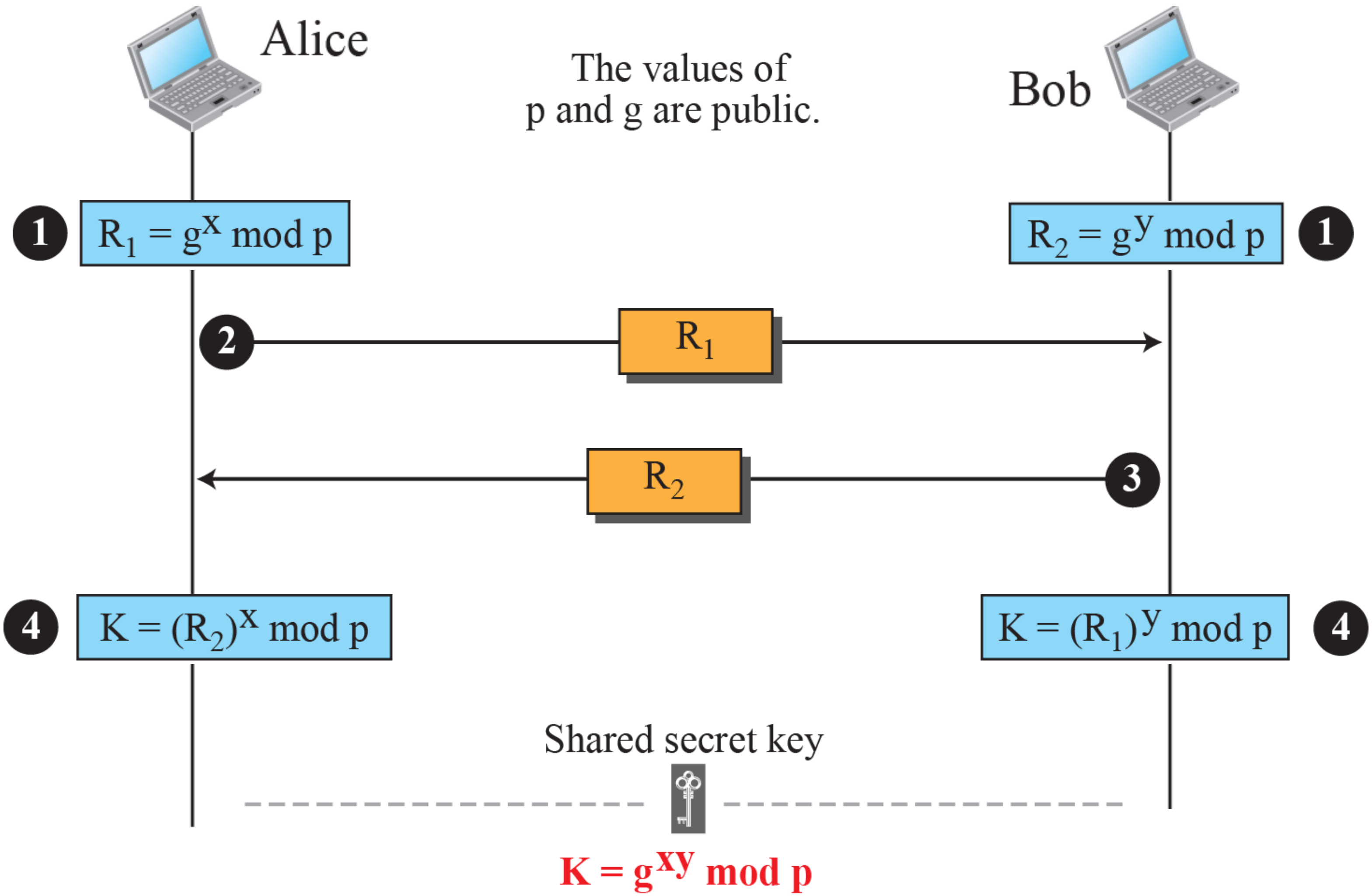
Key Management

- We discussed symmetric-key and asymmetric-key cryptography in the previous sections.

- However, we have not yet discussed how secret keys in symmetric-key cryptography, and public keys in asymmetric-key cryptography, are distributed and maintained.



Creating a session key using KDC



Diffie-Hellman method

Example

- Let us give a trivial example to make the procedure clear. Our example uses small numbers, but note that in a real situation, the numbers are very large.

- Assume that $g = 7$ and $p = 23$. The steps are as follows:

1. Alice chooses $x = 3$ and calculates $R1 = 7^3 \bmod 23 = 21$.
   Bob chooses $y = 6$ and calculates $R2 = 7^6 \bmod 23 = 4$.

2. Alice sends the number 21 to Bob.

Example (continued)

3. Bob sends the number 4 to Alice.

4. Alice calculates the symmetric key K = 4^3 mod 23 = 18.
   Bob calculates the symmetric key K = 21^6 mod 23 = 18.

Conclusion:

- The value of K is the same for both Alice and Bob; g^{xy} mod p = 7^{18}mod 23 = 18.