UNIVERSIDAD
NACIONAL
DE COLOMBIA

Introduction to Cryptography and Information Security

Cryptography Fundamentals

Jeisson Andrés Vergara Vargas, M.Sc.
Departamento de Ingeniería de Sistemas e Industrial
http://javergarav.academy/
javergarav@unal.edu.co

2018-II

Goals

Cryptography

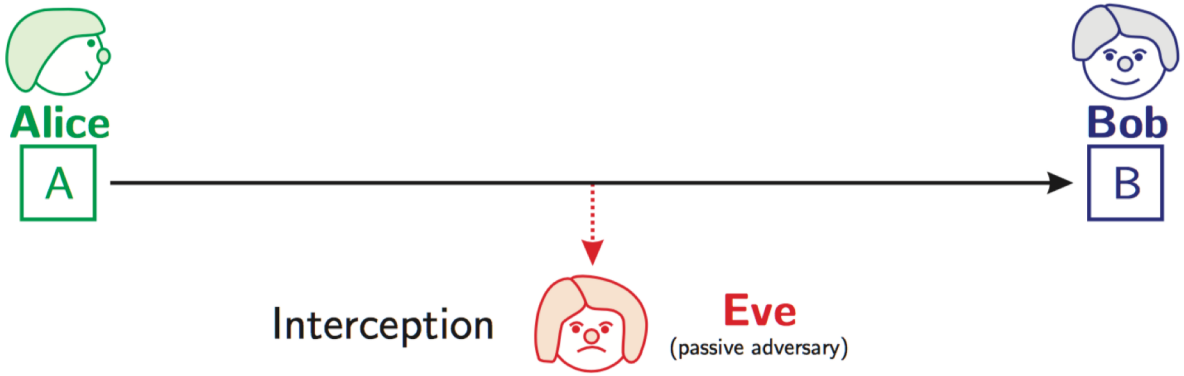
- "Communication in the presence of adversaries". (RONALD RIVEST)
- "An intellectual battle between a code-maker and a code-breaker". (SIMON SINGH)
- "The study of math techniques to meet the fundamental objectives of information security". (HANDBOOK OF APPLIED CRYPTOGRAPHY)

The origin of the word **cryptography** lies in ancient Greek:

$$\underset{\text{(hidden)}}{\text{Κρυπτο}} - \underset{\text{(to write)}}{\text{γραφια}} = \text{to write secret(ly)}$$

Goals of Cryptography

Confidentiality



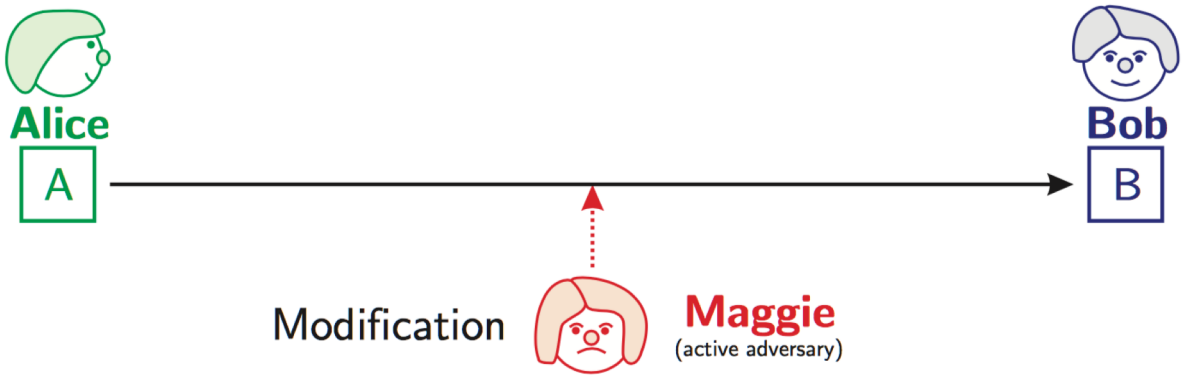
"Prevent unauthorized access"

This comprises two separate requirements:

- Observer cannot **access** the **contents** of the message.
- Observer cannot **identify** the **sender** and **receiver**.

Goals of Cryptography

Integrity



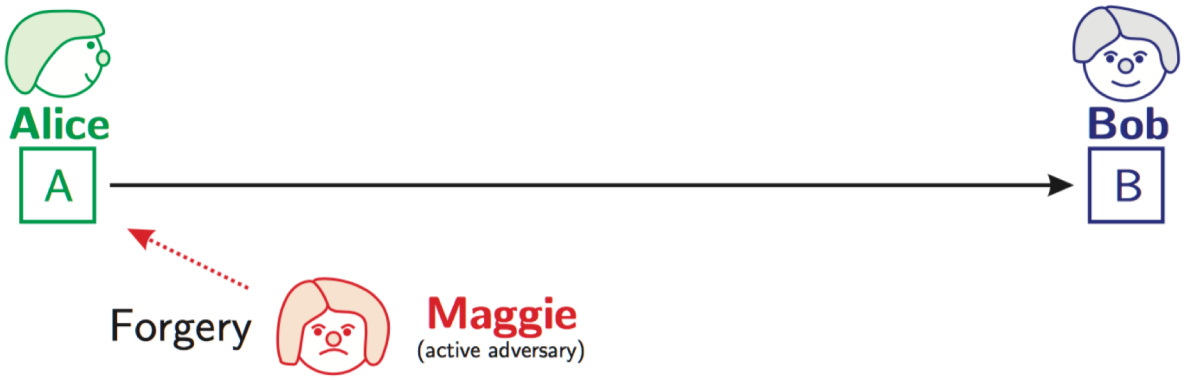
"No modification of existing information"

This requires that the recipient can be sure that:

- The message has not been **changed** or lost during transmission.
- The message has not been **prevented** from reaching the recipient.
- The message has not **reached** the recipient twice.

Goals of Cryptography

Authentication



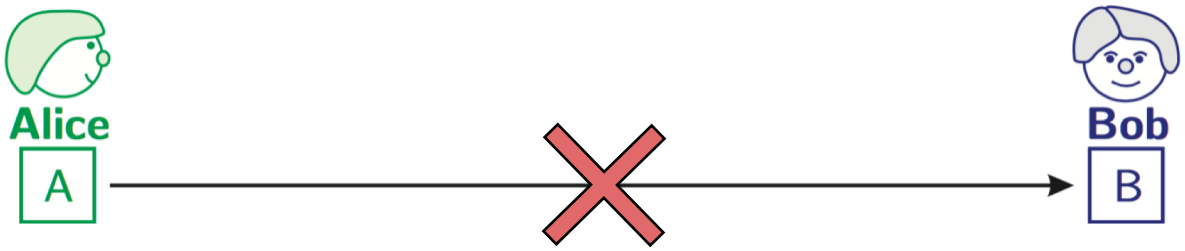
"Identifying either entities or data origins"

This comprises two separate requirements:

- The **sender** can be sure that the message reaches the **intended recipient**, and only the **intended recipient**.
- The **recipient** can be sure that the message came from the **sender** and not an **imposter**. The act by an imposter of sending such a message is referred to as **'spoofing'**.

Goals of Cryptography

Availability



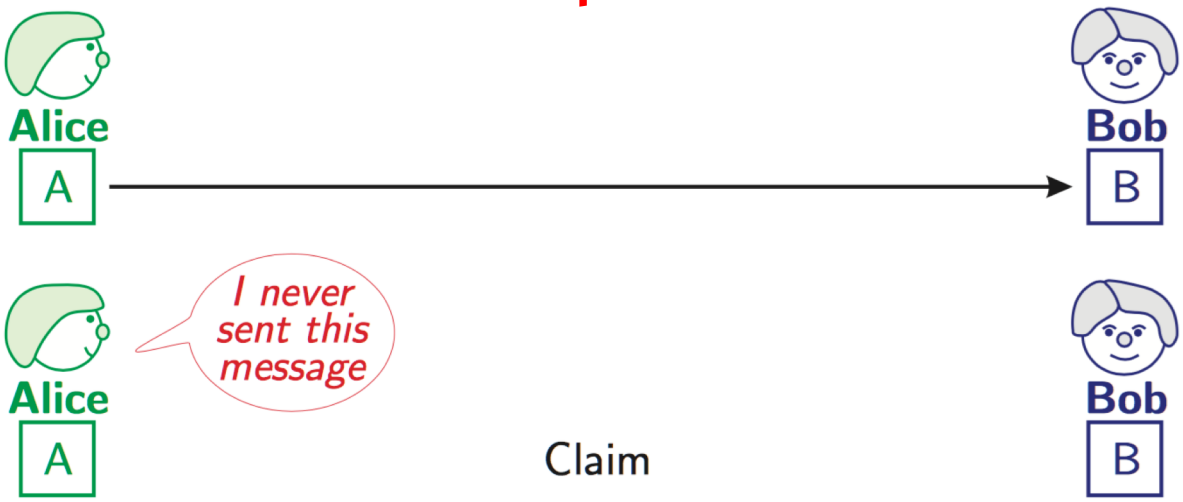
"Information must be available when is needed"

This requires that the following items must be functioning correctly:

- The **computing systems** used to store and process the information.
- The **security controls** used to protect the information.
- The **communication channels** used to access the information.

Goals of Cryptography

Non-Repudiation



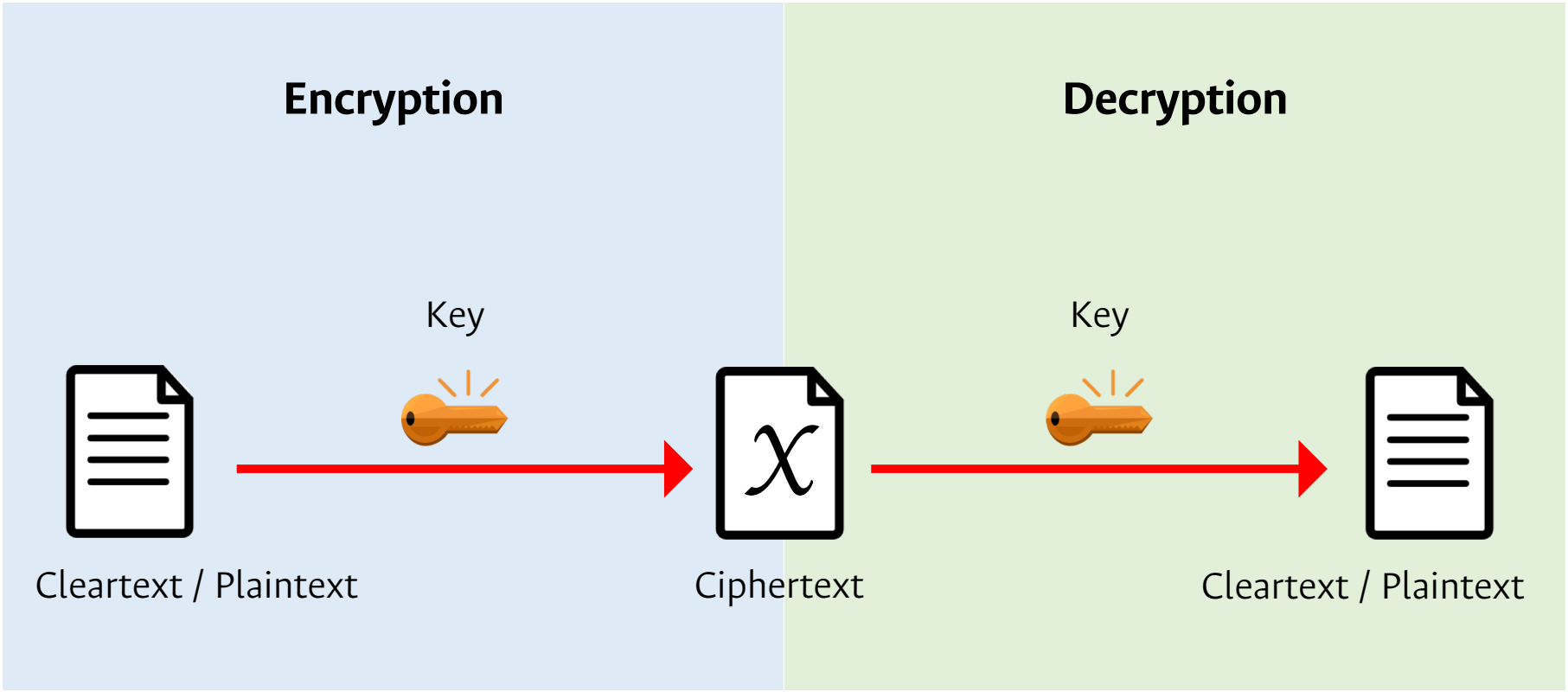
"Preventing denials of messages sent"

This requires that:

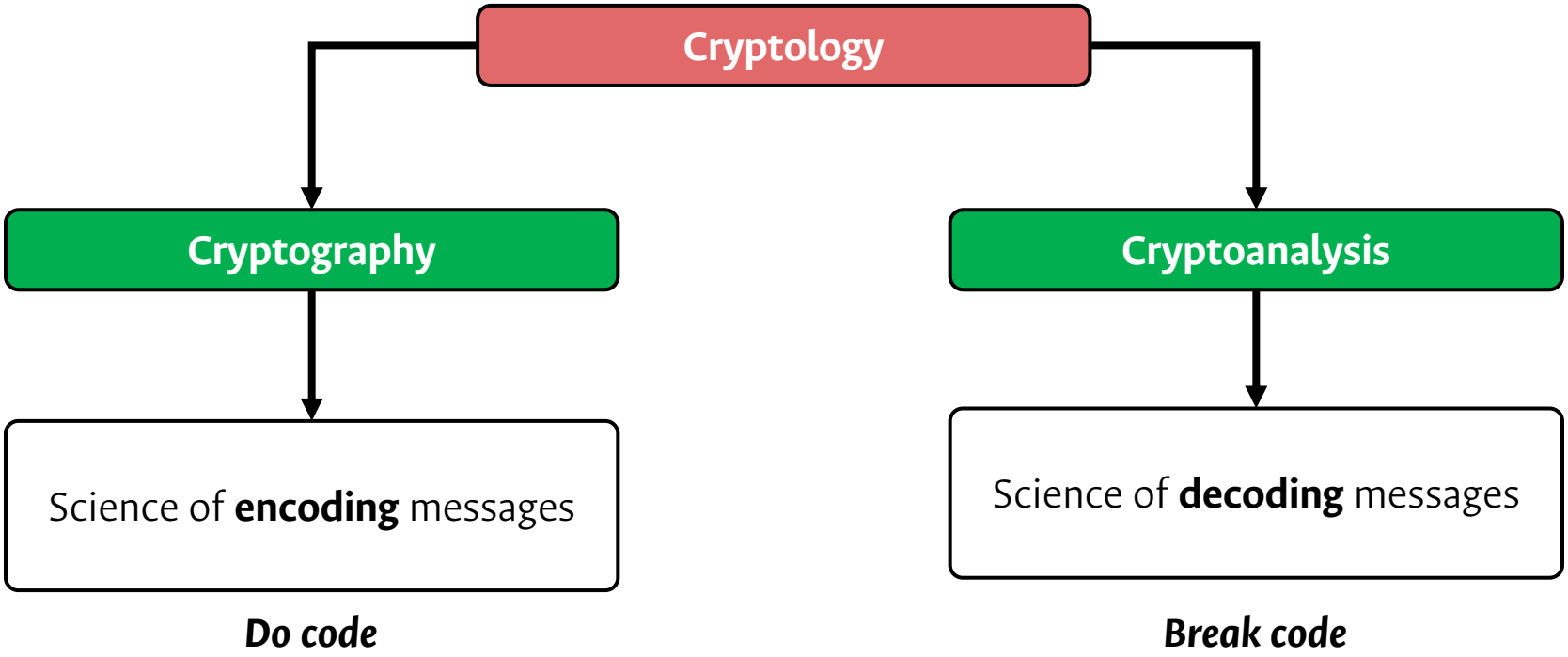
- The **sender cannot credibly deny** that the message was **sent** by them.
- The **recipient cannot credibly deny** that the message was **received** by them.

Terminology

Terminology



Terminology



Common Players

Alice 	Good guys. Generally **Alice** wants to send a message to **Bob**.
Bob 	
Eve	An eavesdropper, she is a passive attacker.
Maggie 	Malicious attacker (sometimes **Mallory**), she is an active attacker; unlike Eve, Maggie can modify messages, substitute his own messages, replay old messages, and so on.
Peggy	A prover.
Victor	A verifier.

One-Time Pad (OTP)

One-Time Pad (OTP) Algorithm

One–Time Pad is a very simple **Polyalphabetic Encryption Algorithm** in which the **key** that encrypts and decrypts is a block of random data called **pads** that cannot be reused. This pad must be at least as long as the plaintext message.

- **Plaintext**: a binary string of length n.
- **Key**: a sequence of random bits of length n.
- **Encryption**: exclusive-or of the plaintext and the key.
- **Decryption**: exclusive-or of the ciphertext and the key.

One-Time Pad (OTP) Algorithm

a	b	$c = a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Exclusive-Or *is equivalent to addition modulo 2.*

One-Time Pad (OTP) Algorithm

Example

Encryption

plaintext	0 1 0 0 0 1 1 0 0 1 0 1 0 1 0 1 0 0 1 1 1 0
key	0 1 0 1 0 0 0 1 1 0 0 1 0 0 1 1 1 0 0 0 0 0 0 1
ciphertext	0 0 0 1 0 1 1 1 1 1 0 0 0 1 1 0 1 1 0 0 1 1 1 1

Decryption

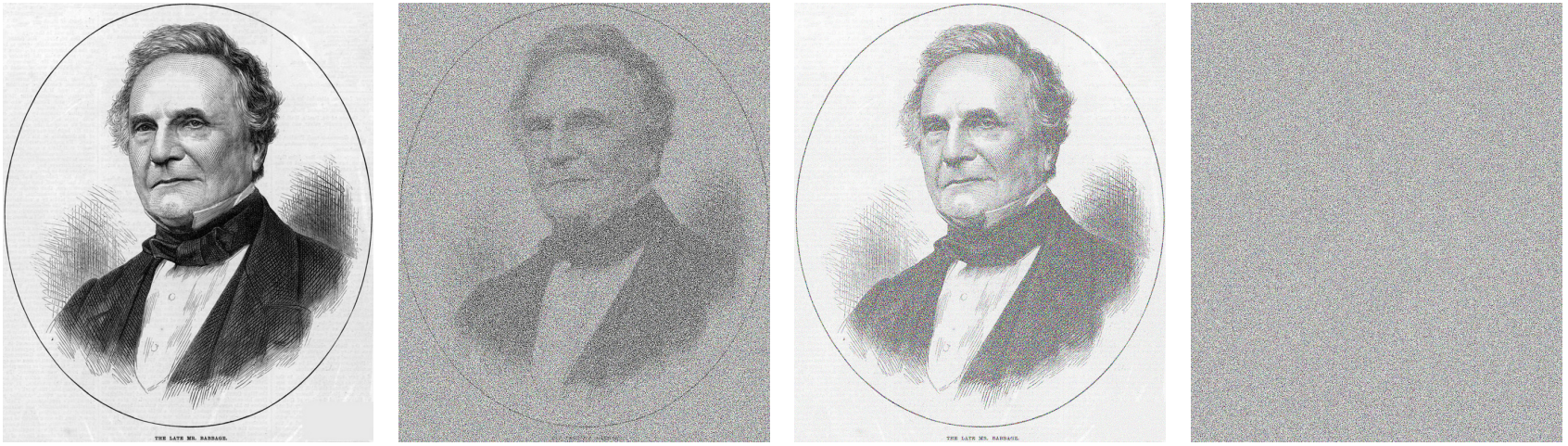
ciphertext	0 0 0 1 0 1 1 1 1 1 0 0 0 1 1 0 1 1 0 0 1 1 1 1
key	0 1 0 1 0 0 0 1 1 0 0 1 0 0 1 1 1 0 0 0 0 0 0 1
plaintext	0 1 0 0 0 1 1 0 0 1 0 1 0 1 0 1 0 0 1 1 1 0

The message corresponds to the binary representation of the text **FUN**.

One-Time Pad (OTP) Algorithm

Why XOR?

Original **AND** **OR** **XOR**



The same image encrypted with the logical operators **AND**, **OR** and **XOR**.

Class Exercise

Instructions

1. Assign each letter a numerical value: **A** = 0, **B** = 1, **C** = 2, ..., **Z** = 25.
2. Take the plaintext as **HELLO**.
3. Take the key as the first five letters of your name.
4. Encrypt the plaintext.
5. Decrypt the ciphertext.

Time: 20 minutes.

Class Exercise

(Mod 26)

A = 0, B = 1, C = 2, ...

Encryption

Plaintext	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)
Key	9 (J)	4 (E)	8 (I)	18 (S)	18 (S)
Ciphertext	16 (Q)	8 (I)	19 (T)	3 (D)	6 (G)

Decryption

Ciphertext	16 (Q)	8 (I)	19 (T)	3 (D)	6 (G)
Key	9 (J)	4 (E)	8 (I)	18 (S)	18 (S)
Ciphertext	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)

Notice that there are $\mathbf{26^5}$ (**11.881.376**) possible keys of length **5**, each with the same probability ($\mathbf{26^{-5}}$) of being picked.

One-Time Pad (OTP) Algorithm

Advantages

- **Easy** to **encrypt** and **decrypt**.
- **Hard** to **break** (theoretically unbreakable).

Disadvantages

- Key must be as long as the plaintext.
- Key distribution and management is difficult to accomplish.
- Key can only be used once.

Perfect Secrecy

In the 1940's **Claude Shannon** introduced the term **perfect secrecy** stating that

"The ciphertext should leak NO information whatsoever about the plaintext, regardless of its distribution".

More formally: $P[M = m \mid C = c] = P[M = m]$

Where **M** and **C** represent the random variables taking the value of the actual message and ciphertext, respectively.

- The **OTP** is effectively the only example of a perfect secrecy (unbreakable) cipher.
- It is impossible to guarantee the security of a cipher system even it is **theoretically secure**, it may be **insecure in practice**.

Kerckhoffs' Principle

In the 1883, **Auguste Kerckhoffs** stated that

"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge".

Some **advantages** of open cryptographic design are:

- Public scrutiny leads to higher confidence.
- No need to protect against reverse engineering.
- Standards can be established.

Bibliography

- [**PINZÓN**] Y. Pinzón, Cryptography. 2014.
- [**DELFS**] H. Delfs and H. Knebl, Introduction to Cryptography, 3rd ed. 2015.