

# Codes and Cryptography

Jorge L. Villar

MAMME, Fall 2015

## PART I

## Structure of the Course

**PART I: Codes** (24 hours)

Simeon Ball

First Exam: **29th October**

**PART II: Cryptography** (28 hours)

Jorge Villar / Javier Herranz

Second Exam: **23rd December**

Final Exam (only if necessary): **8th January**

More information at:

- <http://mamme.masters.upc.edu/>
- <https://fme-intranet.upc.edu/tmp/consgd/cursactual/34954-e-3.pdf>
- [http://www-ma4.upc.edu/~jvillar/crypto\\_course/](http://www-ma4.upc.edu/~jvillar/crypto_course/)
- <http://atenea.upc.edu/>

## Outline

1 Structure of the course

2 Introduction

## Outline

1 Structure of the course

2 Introduction

## Introduction

The main topic:

**Efficient and Reliable Data Transmission and Storage**

e.g.: Binary Data Storage

**Data:** digital data source = (infinite) sequence of binary or  $q$ -ary symbols

**Reliable:** against

- imperfect environment → **Information Coding**
- malicious users → **Cryptography**

**Efficient:** w.r.t.

- read / write / modify / delete time (per bit / per access)
- physical space
- life of stored data

## Example: Binary Data Storage (II)

Reliable against malicious users → **Cryptography**

Confidentiality: Use symmetric encryption

Integrity: Use message authentication codes

Availability: Use secret sharing schemes

## Example: Binary Data Storage (I)

Reliable against imperfect environment → **Information Coding**

Add redundancy (w/o degrading efficiency too much)

- Use error correction codes: detect/correct a few errors
- Use data shuffling: protects against correlated error locations (Compact Disk)

Efficient w.r.t. physical space → **Information Coding**

Use a compression code (w/o degrading speed too much)

## Codes and Cryptography

Jorge L. Villar

MAMME, Fall 2015

**END OF PART I**