

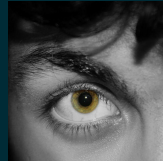
Cryptography

Gaspare Ferraro

March 21, 2019



Visit us!
zenhack.it



@GaspareG
ferraro@gaspa.re

Table of Contents

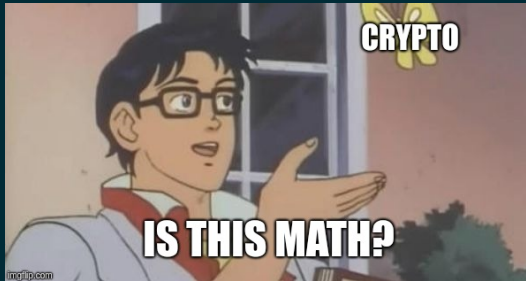
- ▶ 1. Introduction
- ▶ 2. Message encoding
- ▶ 3. Classical cryptography
- ▶ 4. Symmetric-key cryptography
- ▶ 5. Public-key cryptography
- ▶ 6. Hash function
- ▶ 7. Steganography

Part I

Introduction

Warning!

In questo incontro si fa uso della *matematica*!



Non è sempre stato così però...

Why cryptography?

Part II

Message encoding

What is a message?

ASCII encoding

Unicode encoding

Base64

Base6536

Part III

Classical cryptography

Caesar cipher

ROT13

Substitution cipher

Cryptanalysis

Part IV

Symmetric-key cryptography

Symmetric-key cryptography

Shannon principle

XOR cipher

Part V

Public-key cryptography

Part VI

Hash function

Part VII

Steganography