Cryptography

Hackers ahead of time

Gaspare Ferraro
ferraro@gaspa.re

November 15, 2018

Visit us!

@GaspareG

Part I

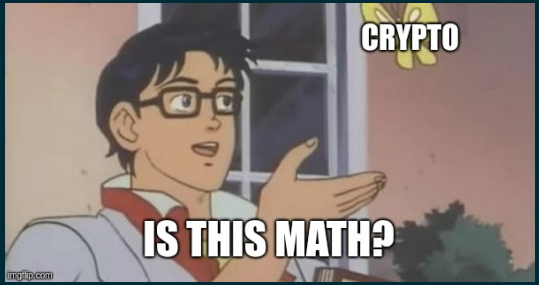
Introduzione

Warning!

In questo incontro si fa uso della *matematica*!

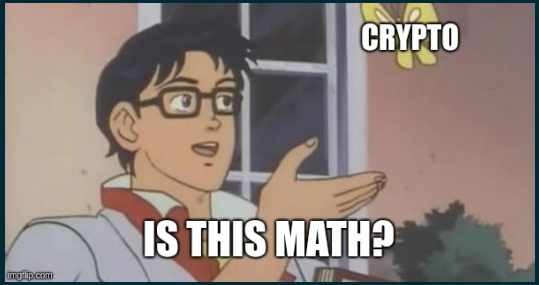
Warning!

In questo incontro si fa uso della *matematica*!



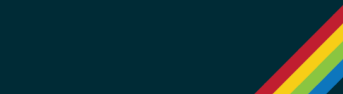
Warning!

In questo incontro si fa uso della *matematica*!



Non è sempre stato così però...

La crittografia ieri



La crittografia ieri

(c) Cifrario di Cesare

La crittografia ieri

(e) Cifrario di Cesare

(f) Scitala

La crittografia oggi

Le necessità, così come le risorse a disposizione, si sono evolute
ed oggi possiamo suddividere la crittografia in:

La crittografia oggi

Le necessità, così come le risorse a disposizione, si sono evolute ed oggi possiamo suddividere la crittografia in:

(DE|EN)CRYPTION	**ASYMETRIC (RSA, ECC, ...)** **SYMMETRIC (DES, AES, ...)**
KEY EXCHANGE	**RSA, DH, ECDH, ...**
AUTHENTICATION	**RSA, DSA, ECDSA, ...**
HASHING	**MD5, SHA-1, SHA-256, ...**

Part II

Crittografia simmetrica

Part III

Crittografia asimmetrica

Part IV

Hashing