Cryptography

A (nearly) complete overview

Gaspare Ferraro

March 22, 2019

Visit us!
zenhack.it

@GaspareG
ferraro@gaspa.re

Table of Contents

Table of Contents

Warning!

Why cryptography?

Cryptography yesterday

Cryptography today

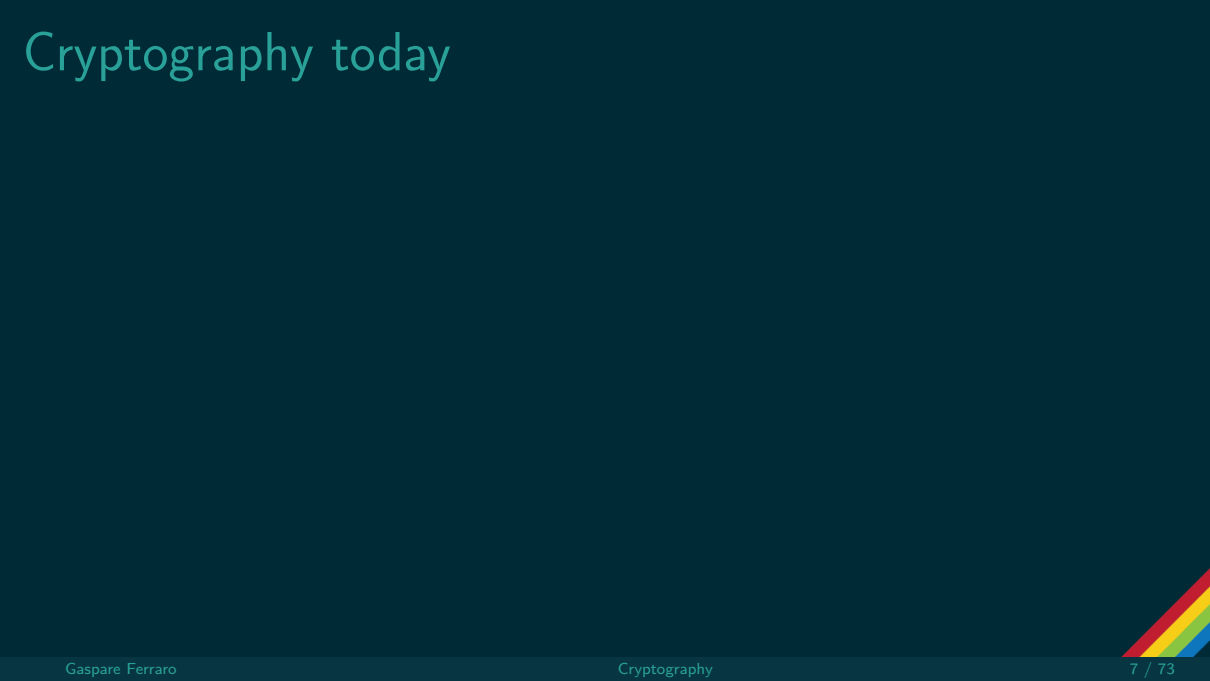


Table of Contents

What is a message?

ASCII encoding

Unicode encoding

Base64

Base65536

Table of Contents

Caesar cipher

ROT13

Substitution cipher

Cryptanalysis

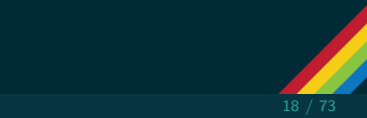


Table of Contents

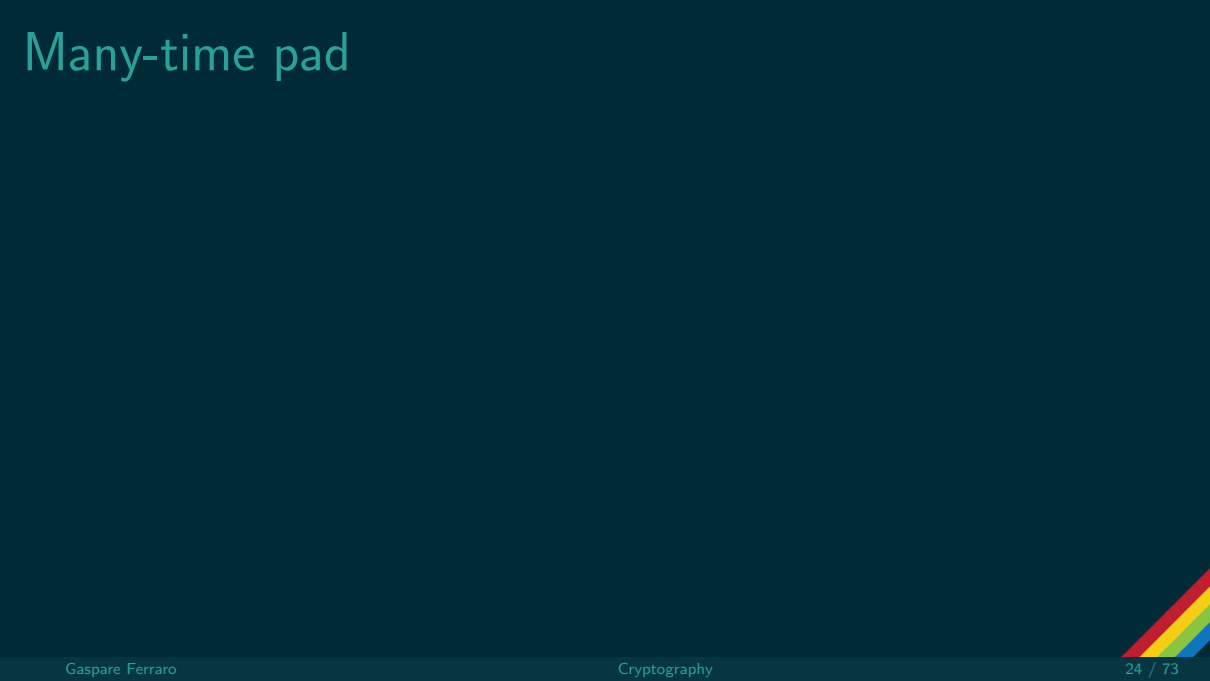
Symmetric-key cryptography

Shannon principle

XOR cipher

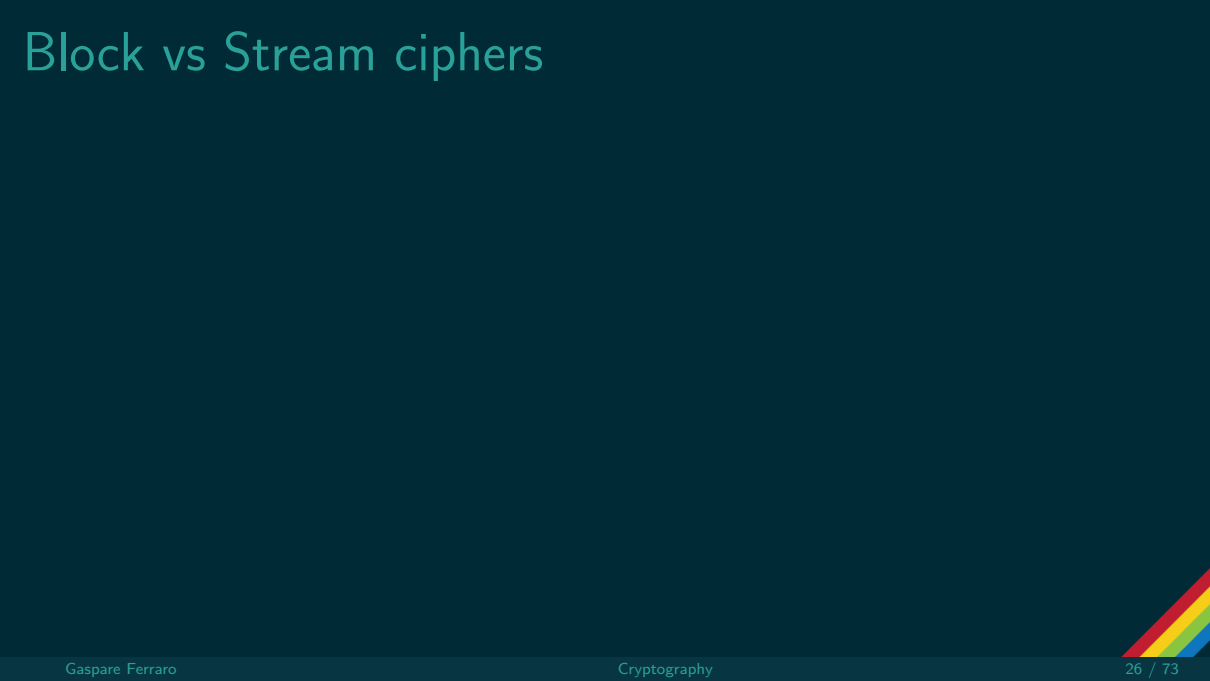
One-time pad

Many-time pad



XorTool

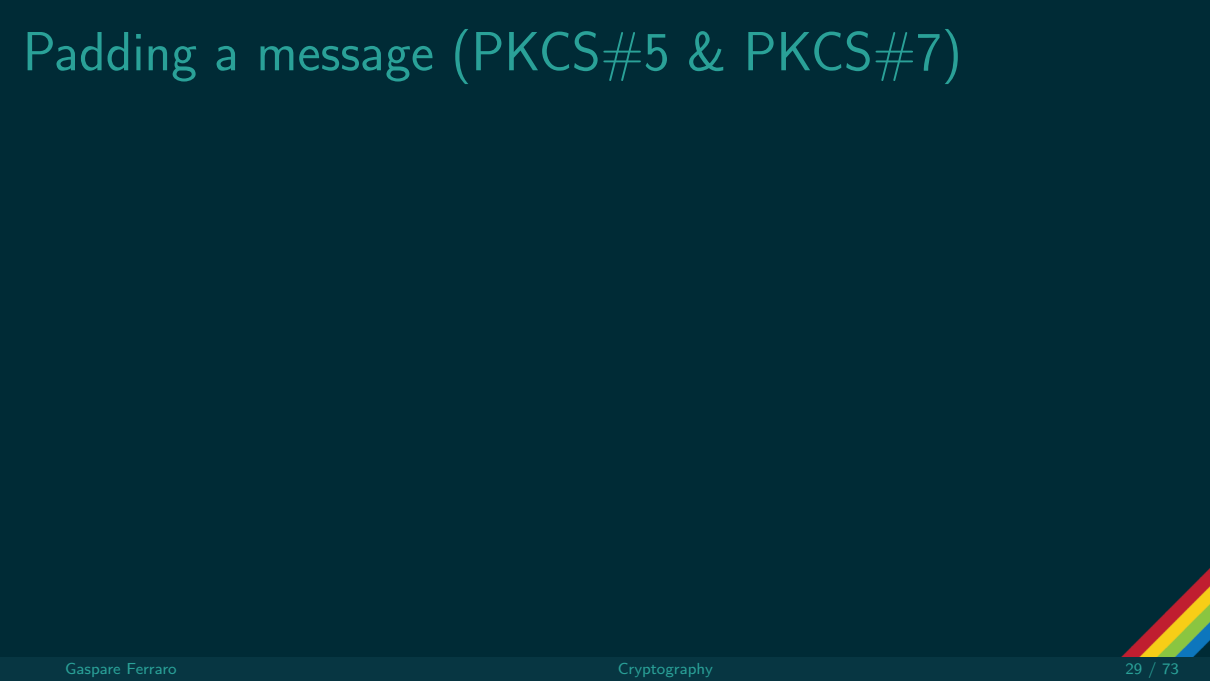
Block vs Stream ciphers



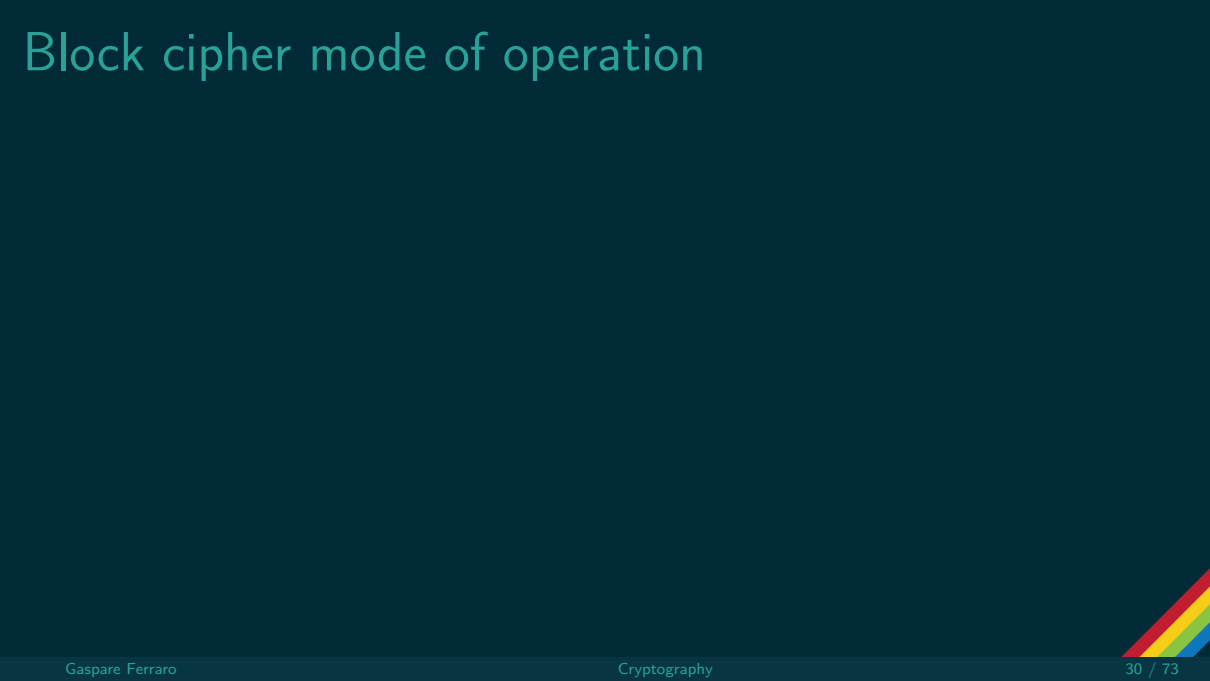
DES

AES

Padding a message (PKCS#5 & PKCS#7)



Block cipher mode of operation



ECB (Electronic Codebook)

How to break ECB (padding-oracle attack)

CBC (Cipher Block Chaining)

How to break CBC (bit-flipping attack)

Stream ciphers (Salsa & Cha-Cha)

Table of Contents

Public-key cryptography

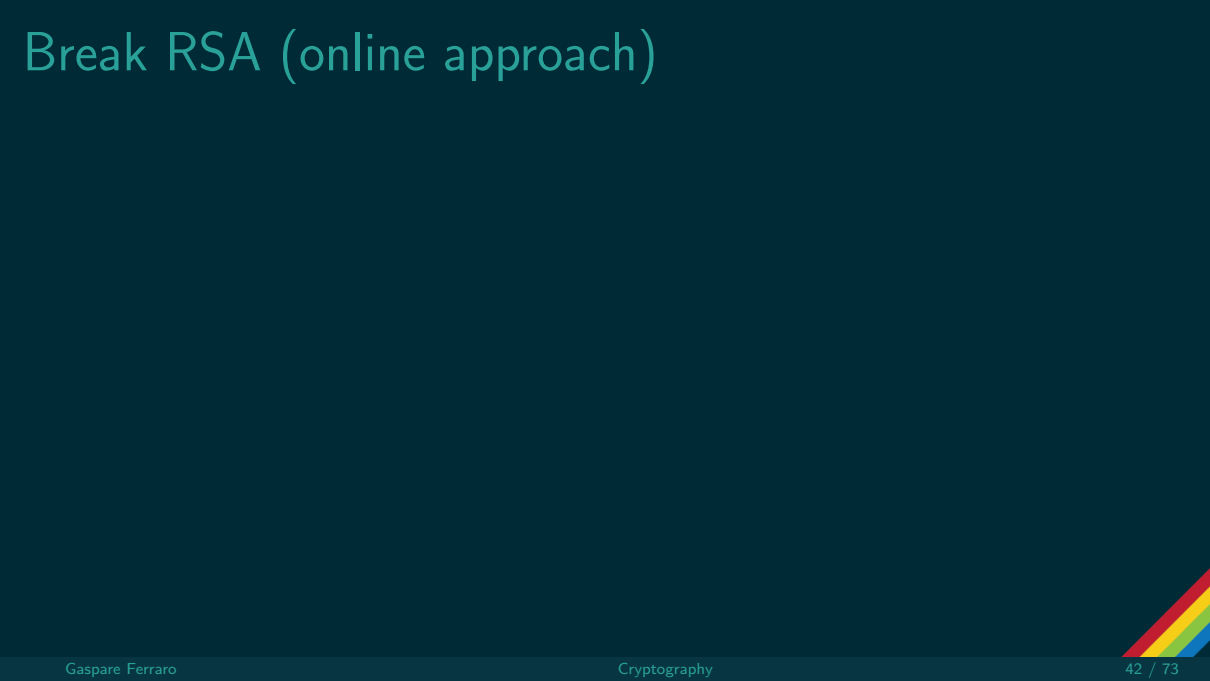
Modular arithmetic

RSA

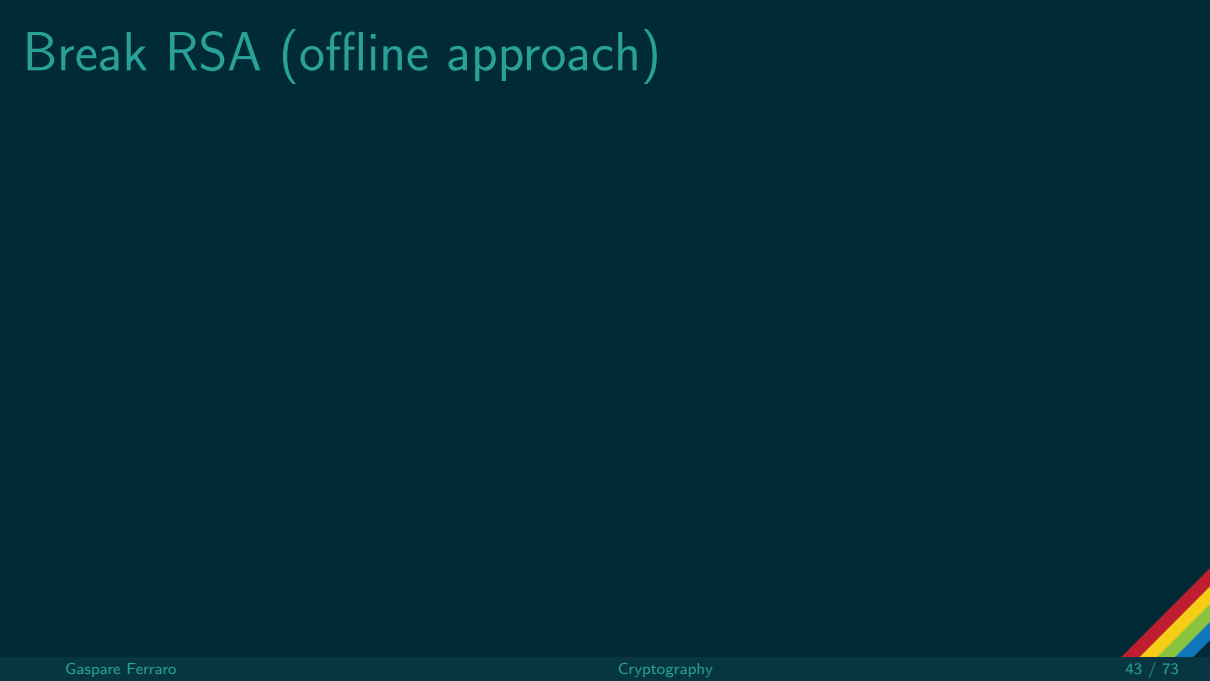
An example...

How to choose parameters

Break RSA (online approach)



Break RSA (offline approach)



Break RSA (online approach)

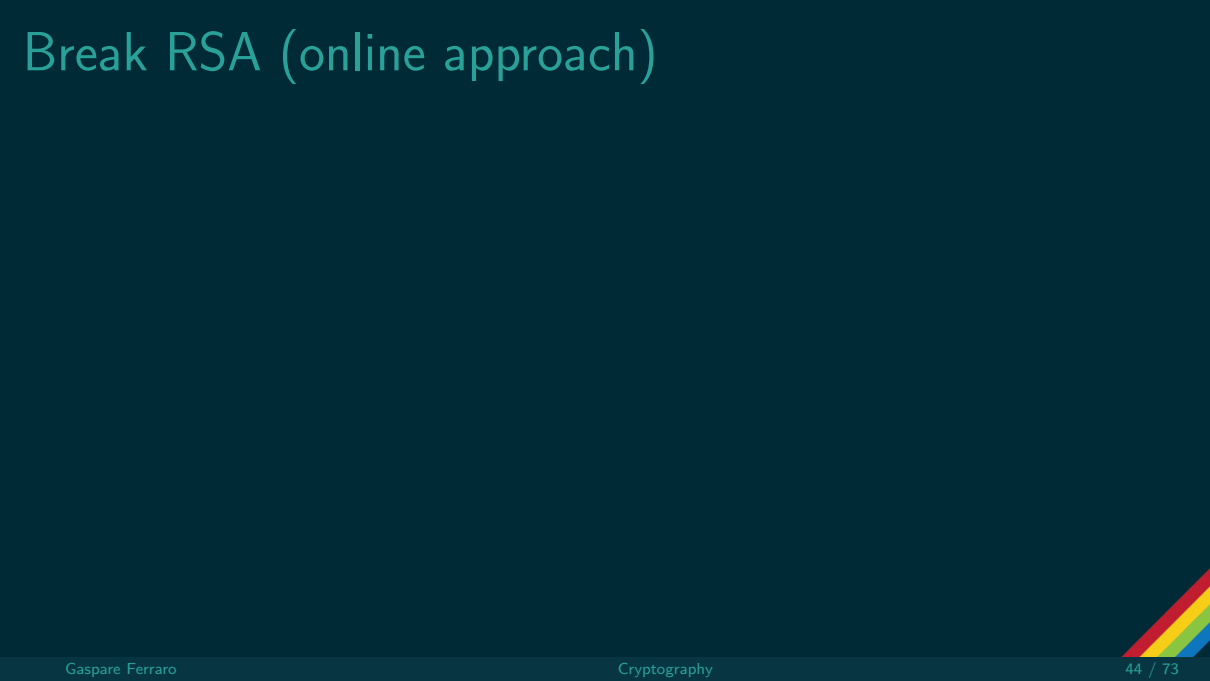


Table of Contents

Key exchange

Diffie-Hellman key exchange

A man-in-the-middle attack to DH

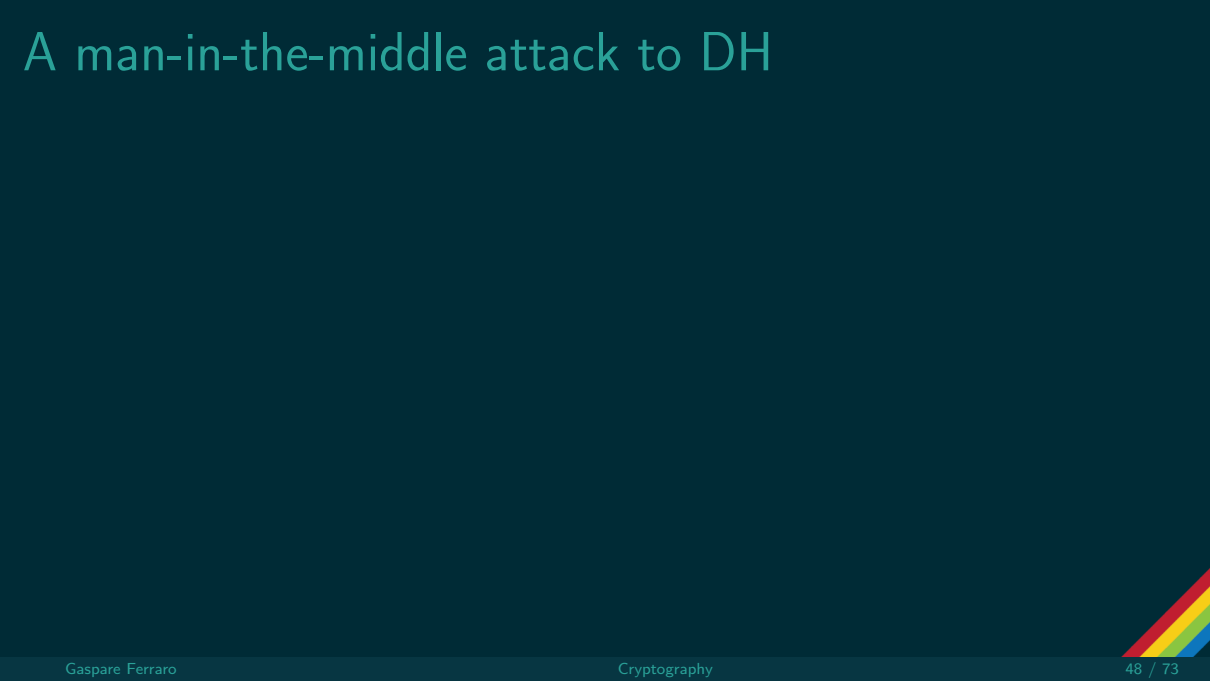


Table of Contents

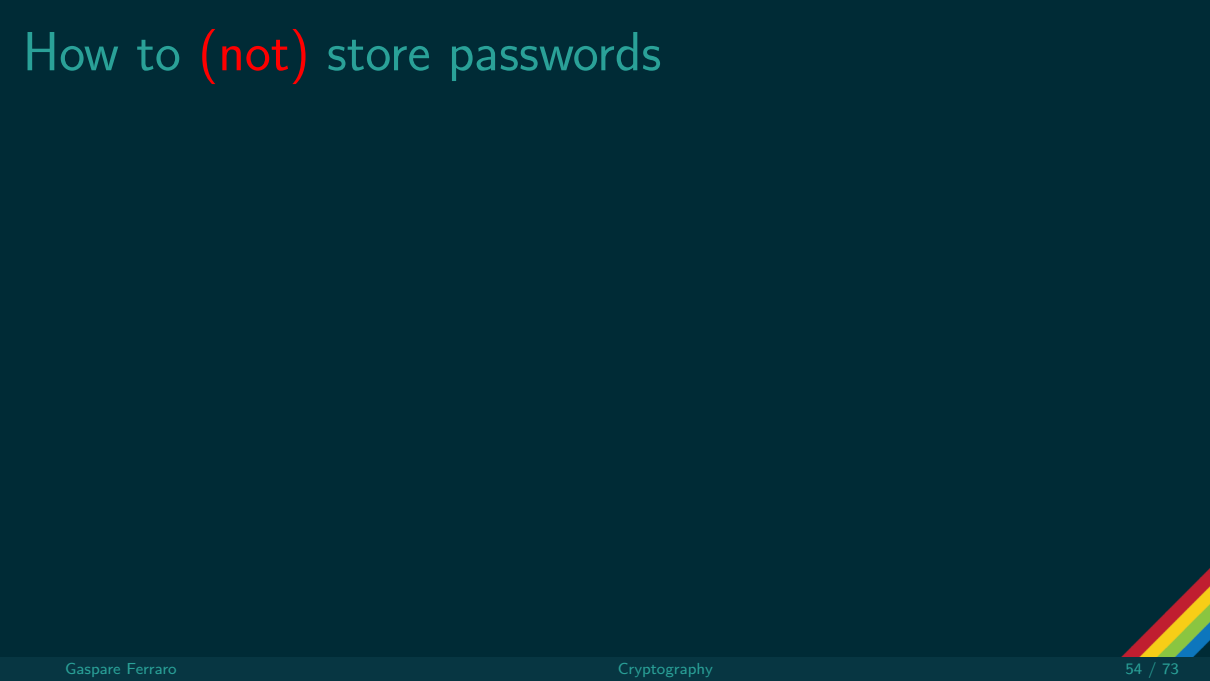
Hash function

Why hash

How to store passwords

How to store passwords[2]

How to (not) store passwords



Proof of Work

MD5

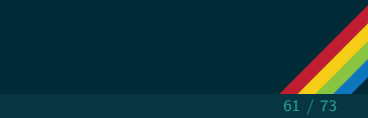
SHA{0, 1, 2}

Finding collision

Reverse an hash function (online approach)

Reverse an hash function (offline approach)

fcrackzip



JohnTheRipper

Hashcat

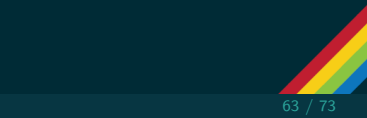


Table of Contents

Steganography

File stego (file, binwalk, exiftool, strings)

Image stego

Layer stego

Audio stego

Morse code

Spectography analysis (Audacity)

AudioStego

DeepSound