

# CyberSecurity: Principle and Practice

*BSc Degree in Computer Science  
2023-2024*

## Lesson 4: Cryptographic Tools pt.1

Prof. Mauro Conti

Department of Mathematics

University of Padua

[conti@math.unipd.it](mailto:conti@math.unipd.it)

<http://www.math.unipd.it/~conti/>

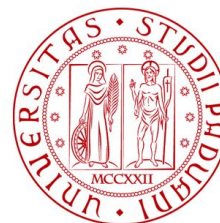
Teaching Assistants

Tommaso Bianchi

[tommaso.bianchi@phd.unipt.it](mailto:tommaso.bianchi@phd.unipt.it)

Riccardo Preatoni

[riccardo.preatoni@studenti.unipd.it](mailto:riccardo.preatoni@studenti.unipd.it)



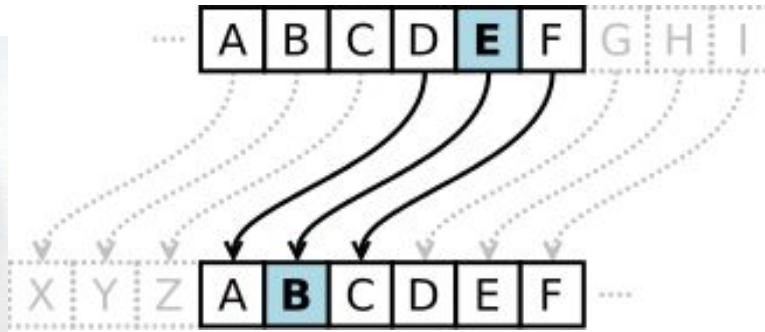
UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA



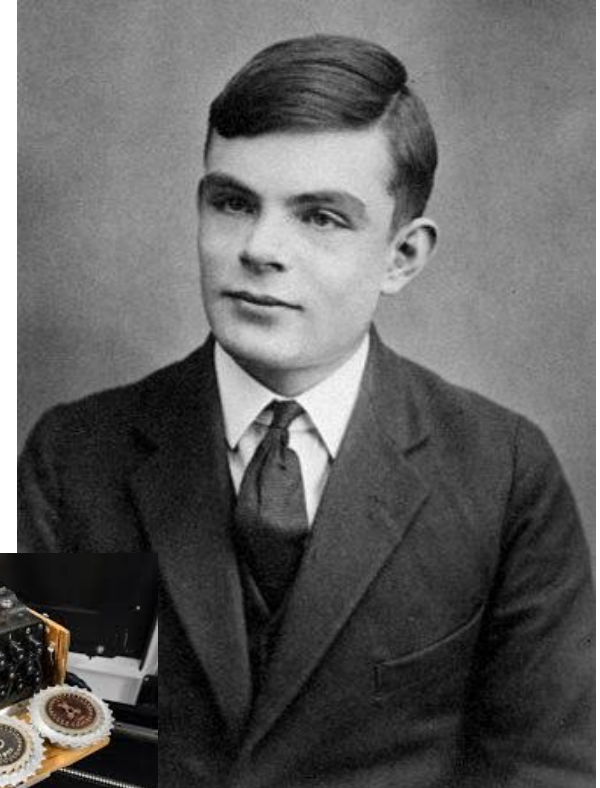
SPRITZ  
SECURITY & PRIVACY  
RESEARCH GROUP



DIPARTIMENTO 1  
**MATEMATICA**



Caesar Cipher: private  
correspondence (~50BC)

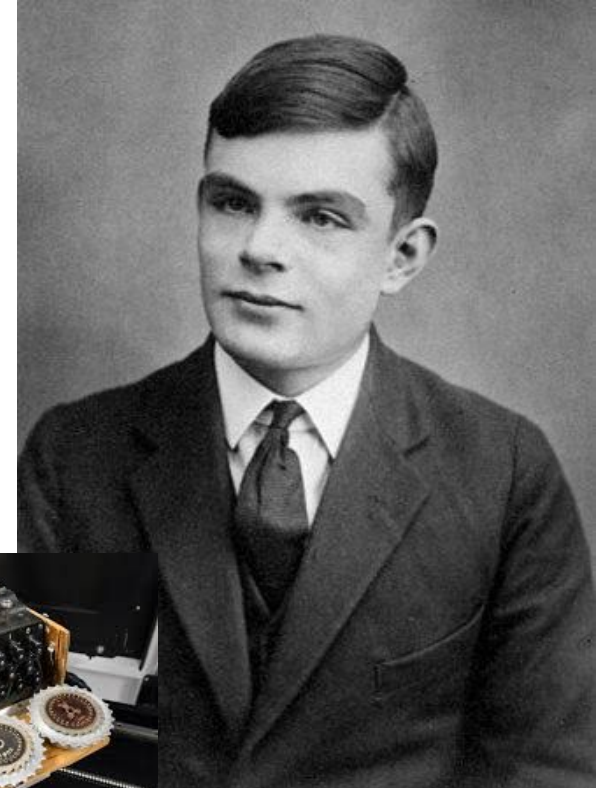
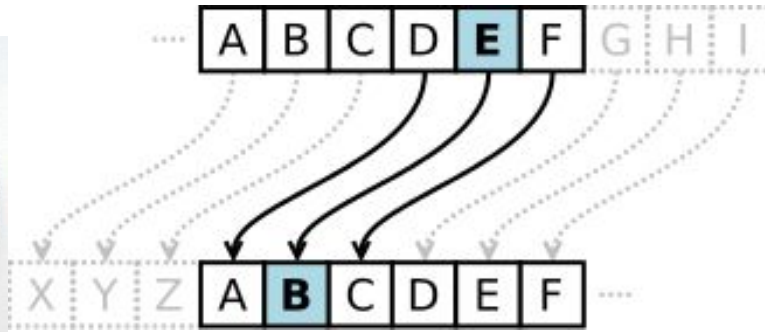


Alan Turing: decryption of German's  
ciphers during WWII (1940s)

# Historical Facts



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA



Cesar Cipher: private  
correspondence (~50BC)



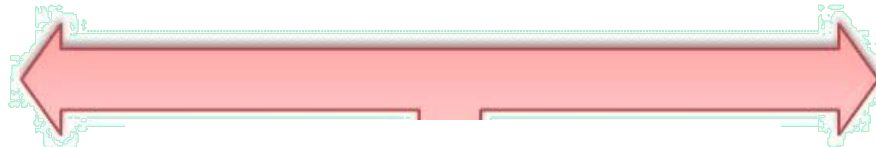
Alan Turing: decryption of German's  
ciphers during WWII (1940s)

- Cryptographic algorithms important element in security services
- Review various types of elements
  - symmetric encryption
  - public-key (asymmetric) encryption
  - secure hash functions
- Example of encryption





# Encryption

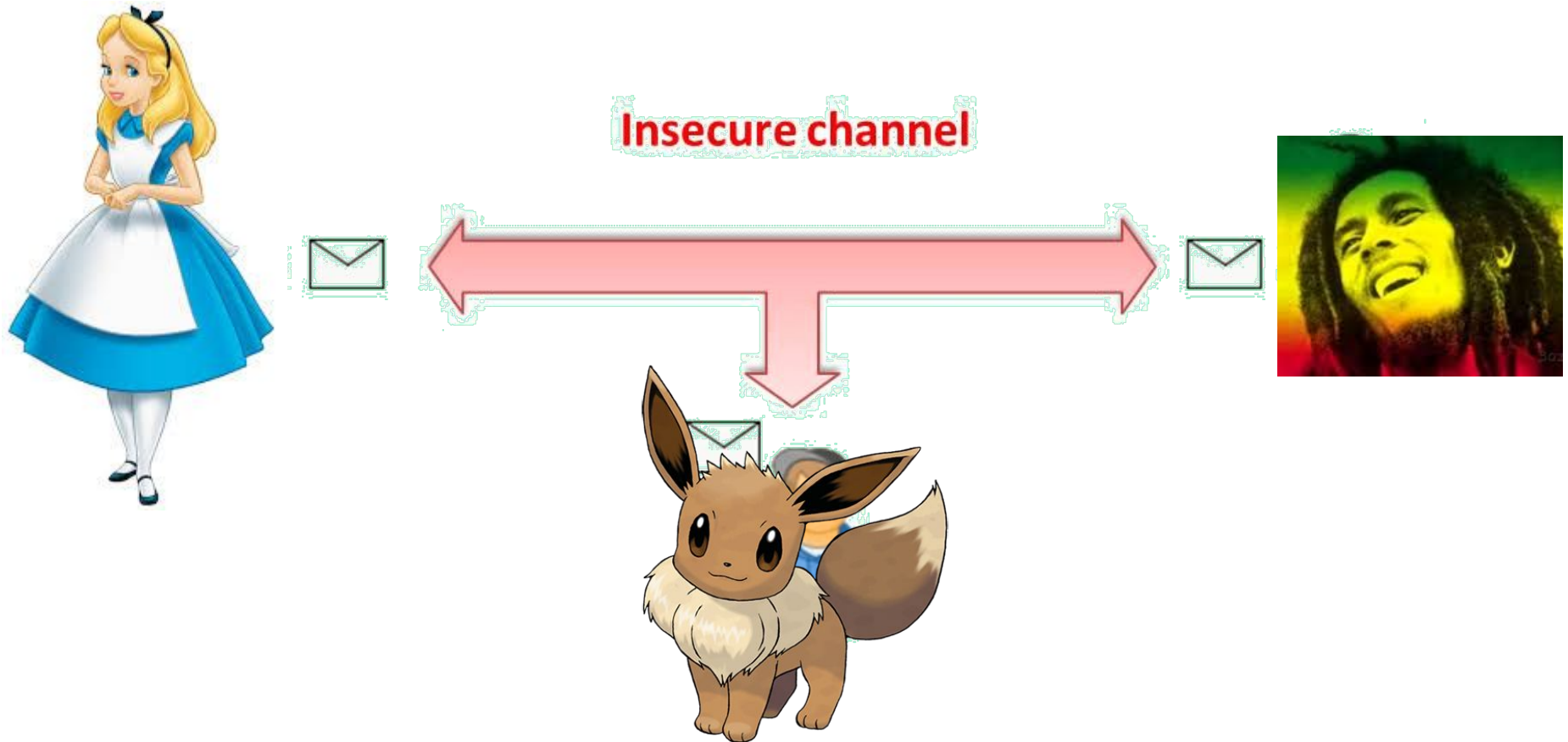


Insecure channel

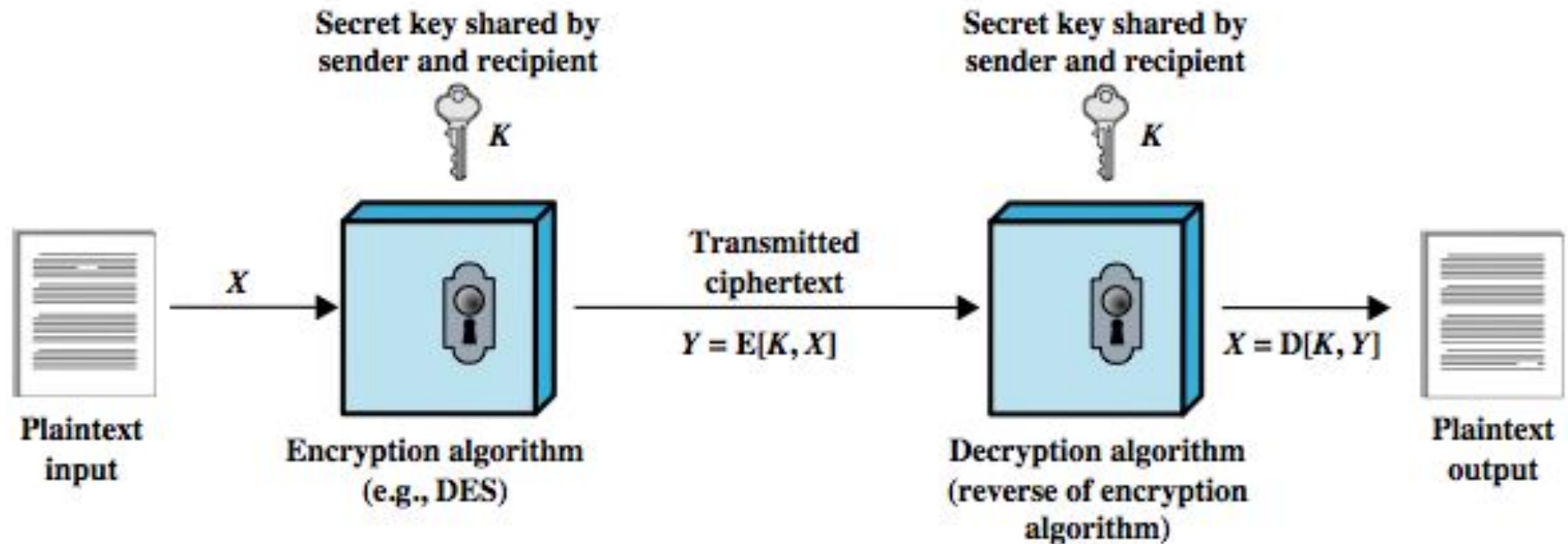




# Encryption



# Symmetric Encryption



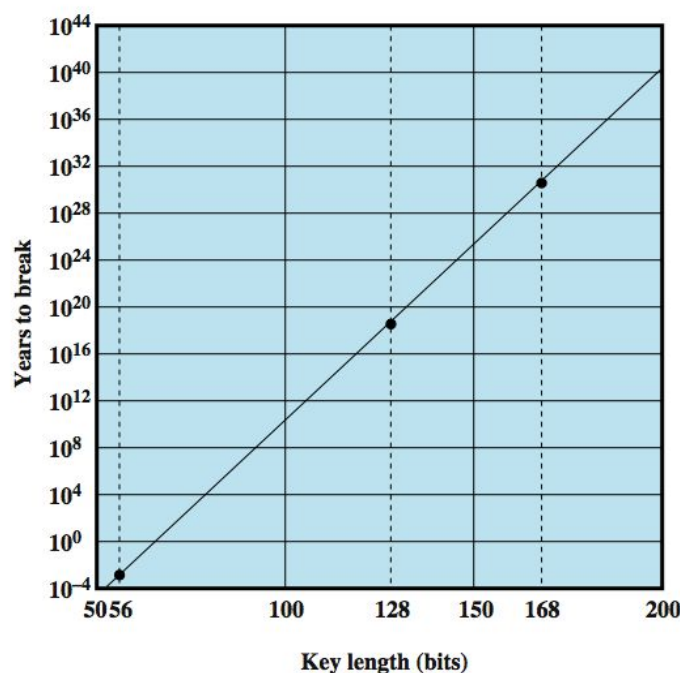


- Cryptanalysis
  - Rely on nature of the algorithm
  - Plus some knowledge of plaintext characteristics
  - Even some sample plaintext-ciphertext pairs
  - Exploits characteristics of algorithm to deduce specific plaintext or key
- Brute-force attack
  - Try all possible keys on some ciphertext until get an intelligible translation into plaintext

# Exhaustive Key Search



| Key Size (bits)             | Number of Alternative Keys     | Time Required at 1 Decryption/ $\mu$ s                            | Time Required at $10^6$ Decryptions/ $\mu$ s |
|-----------------------------|--------------------------------|---|--|
| 32                          | $2^{32} = 4.3 \times 10^9$     | $2^{31} \mu\text{s} = 35.8 \text{ minutes}$                       | 2.15 milliseconds                            |
| 56                          | $2^{56} = 7.2 \times 10^{16}$  | $2^{55} \mu\text{s} = 1142 \text{ years}$                         | 10.01 hours                                  |
| 128                         | $2^{128} = 3.4 \times 10^{38}$ | $2^{127} \mu\text{s} = 5.4 \times 10^{24} \text{ years}$          | $5.4 \times 10^{18} \text{ years}$           |
| 168                         | $2^{168} = 3.7 \times 10^{50}$ | $2^{167} \mu\text{s} = 5.9 \times 10^{36} \text{ years}$          | $5.9 \times 10^{30} \text{ years}$           |
| 26 characters (permutation) | $26! = 4 \times 10^{26}$       | $2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12} \text{ years}$ | $6.4 \times 10^6 \text{ years}$              |



# Symmetric Encryption



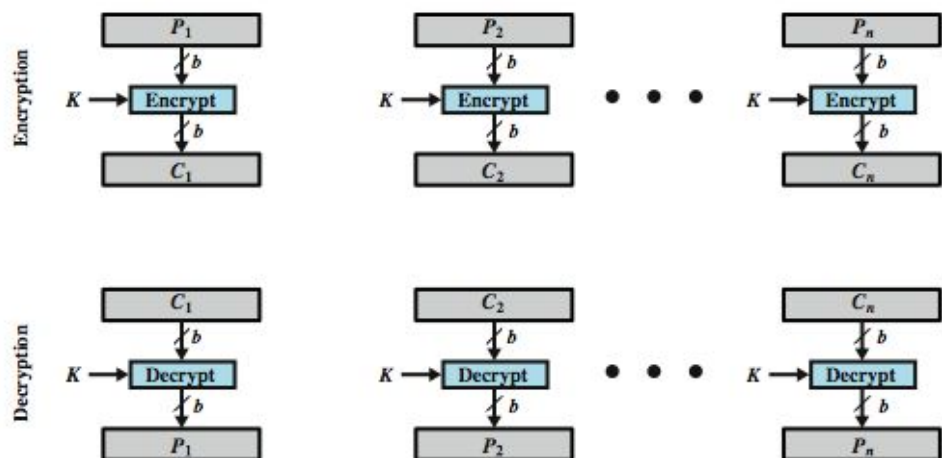
|                              | DES | Triple DES | AES              |
|------------------------------|-----|------------|------------------|
| Plaintext block size (bits)  | 64  | 64         | 128              |
| Ciphertext block size (bits) | 64  | 64         | 128              |
| Key size (bits)              | 56  | 112 or 168 | 128, 192, or 256 |

DES = Data Encryption Standard

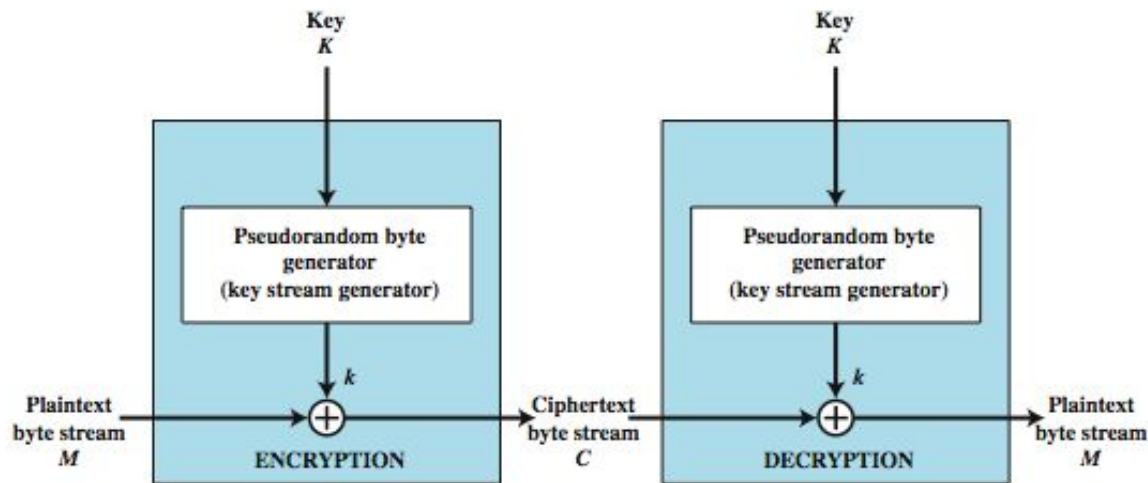
AES = Advanced Encryption Standard

- Data Encryption Standard (DES) is the most widely used encryption scheme
  - Uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block
  - Concerns about algorithm & use of 56-bit key
- Triple-DES
  - Repeats basic DES algorithm three times
  - Using either two or three unique keys
  - Much more secure but also much slower

# Block vs. Stream Ciphers



(a) Block cipher encryption (electronic codebook mod)

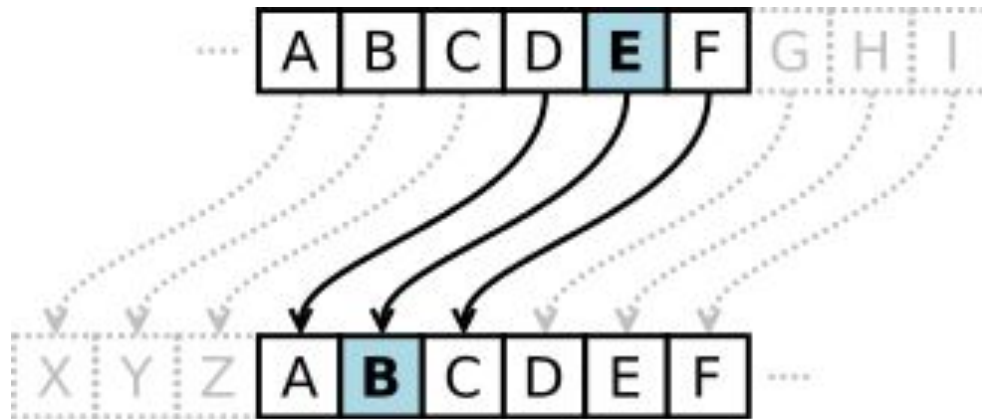


(b) Stream encryption

# Example 1 - Caesar Cipher



- Substitution cipher
  - the alphabet is shifted
  - one of the easiest ciphers (and not really secure)





# Example 1 - Caesar Cipher



- Cyphertext:  
“QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD”

Any ideas?

# Example 1 - Caesar Cipher



- Cyphertext:
  - “QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV  
ALD”
- Solution: try all the possible combinations of alphabets (shifts)
- Cryptanalysis + brute force in this case is easier than cryptanalysis
- Plaintext: “THE QUICK BROWN FOX JUMPS OVER THE  
LAZY DOG”

- XOR is it widely adopted in crypto algorithms
  - Boolean operation
    - $0 \text{ xor } 0 = 0$
    - $0 \text{ xor } 1 = 1$
    - $1 \text{ xor } 0 = 1$
    - $1 \text{ xor } 1 = 0$
  - Represented with the symbol “  $\wedge$  ”
- $\text{enc\_message} = \text{clear\_message} \wedge \text{key}$

## Properties:

- XOR is commutative

$$a \wedge b = b \wedge a$$

- XOR is associative

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

- Anything XORed with itself is zero

$$a \wedge a = 0$$

- Anything XORed with zero is anything

$$a \wedge 0 = a$$

$\text{enc\_message} = \text{clear\_message} \wedge \text{key}$

$\text{clear\_message} = \text{enc\_message} \wedge \text{key}$

$\text{key} = \text{clear\_message} \wedge \text{enc\_message}$

- XOR is used between a key and a message
  - Often  $\text{len}(\text{key}) \ll \text{len}(\text{message})$
  - We “repeat the key” on the message
- Example
  - `clear_message` = “THIS IS A MESSAGE”
  - `key` = “YOU”

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T | H | I | S |   | I | S |   | A |   | M | E | S | S | A | G | E |
| Y | O | U | Y | O | U | Y | O | U | Y | O | U | Y | O | U | Y | O |



# Cryptographic Tools: XOR



|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| T  | H  | I  | S  |    | I  | S  |    | A  |    | M  | E  | S  | S  | A  | G  | E  |
| 84 | 72 | 73 | 83 | 32 | 73 | 83 | 32 | 65 | 32 | 77 | 69 | 83 | 83 | 65 | 71 | 69 |

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Y  | O  | U  | Y  | O  | U  | Y  | O  | U  | Y  | O  | U  | Y  | O  | U  | Y  | O  |
| 89 | 79 | 85 | 89 | 79 | 85 | 89 | 79 | 85 | 89 | 79 | 85 | 89 | 79 | 85 | 89 | 79 |

# Cryptographic Tools: XOR



|     |    |    |    |    |     |    |    |     |    |     |    |    |    |    |    |    |    |
|-----|----|----|----|----|-----|----|----|-----|----|-----|----|----|----|----|----|----|----|
| msg | 84 | 72 | 73 | 83 | 32  | 73 | 83 | 32  | 65 | 32  | 77 | 69 | 83 | 83 | 65 | 71 | 69 |
| key | 89 | 79 | 85 | 89 | 79  | 85 | 89 | 79  | 85 | 89  | 79 | 85 | 89 | 79 | 85 | 89 | 79 |
| enc | 13 | 7  | 28 | 10 | 111 | 28 | 10 | 111 | 20 | 121 | 2  | 16 | 10 | 28 | 20 | 30 | 10 |

The XOR between two integer it is the result of the xor of their binary representations.

- 84 = 1010100
- 89 = 1011001
- 13 = 0001101

Kasiski elimination:

- Technique to attack substitution ciphers
  - E.g., **Vigenère** cipher  
(Polyalphabetic cipher, base on initial idea of **Bellaso**)
- Involve the inspection of character sequences inside a ciphertext
  - We look for anomaly amount of repetitions
  - At least sequences with more than 3 characters
  - An anomaly might be derived by a repetition on the plaintext
- Useful to identify the key length
  - ... and cryptanalysis

## Student @ UniPD ~1537

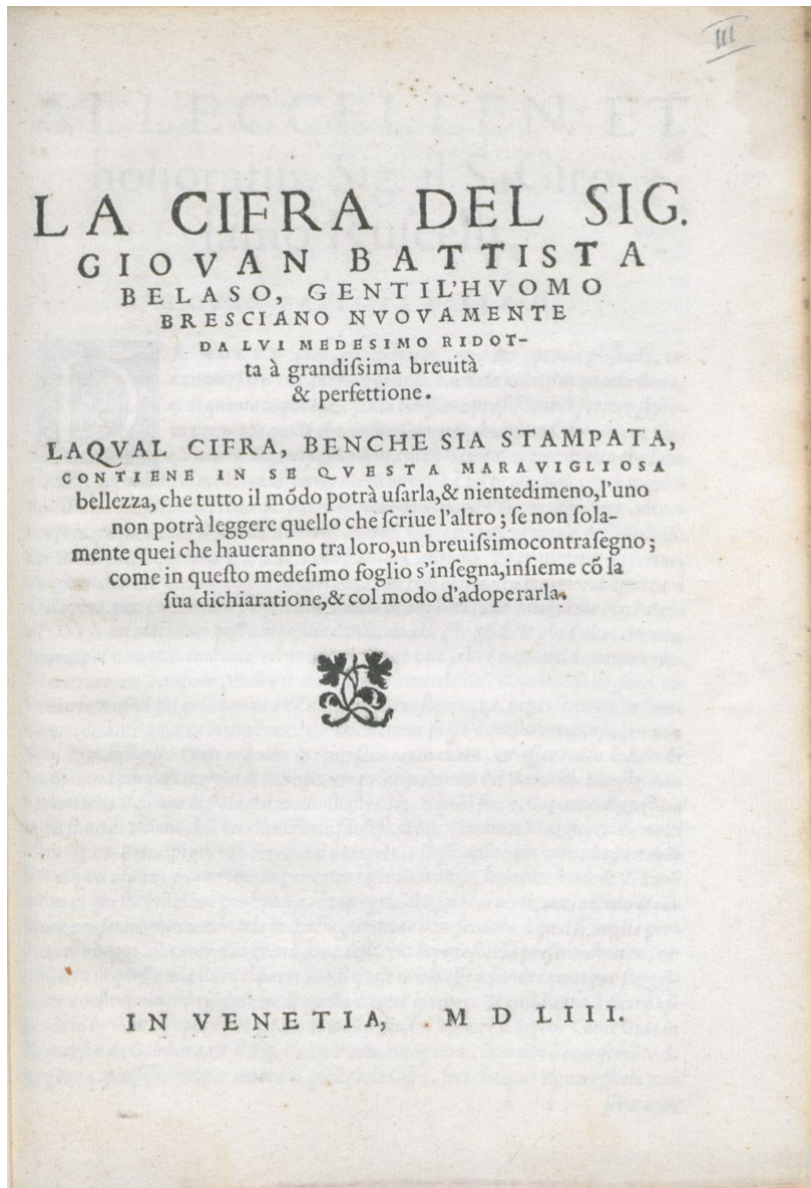
ISTITUTO  
PER LA STORIA DELL'UNIVERSITÀ DI PADOVA

ACTA  
GRADUUM ACADEMICORUM  
AB ANNO 1526 AD ANNUM 1537

A CURA DI  
ELDA MARTELLOZZO FORIN



EDITRICE ANTENORE · PADOVA  
MCMLXX



# XOR - Kasiski Elimination



|    |   |    |    |     |    |    |     |    |     |   |    |    |    |    |    |    |
|----|---|----|----|-----|----|----|-----|----|-----|---|----|----|----|----|----|----|
| 13 | 7 | 28 | 10 | 111 | 28 | 10 | 111 | 20 | 121 | 2 | 16 | 10 | 28 | 20 | 30 | 10 |
|----|---|----|----|-----|----|----|-----|----|-----|---|----|----|----|----|----|----|

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T | H | I | S |   | I | S |   | A |   | M | E | S | S | A | G | E |
| Y | O | U | Y | O | U | Y | O | U | Y | O | U | Y | O | U | Y | O |

# Questions? Feedback? Suggestions?



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

