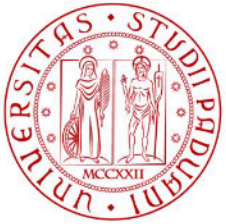
CyberSecurity: Principle and Practice

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

Teaching Assistants
Tommaso Bianchi
tommaso.bianchi@phd.unipt.it
Riccardo Preatoni
riccardo.preatoni@studenti.unipd.it

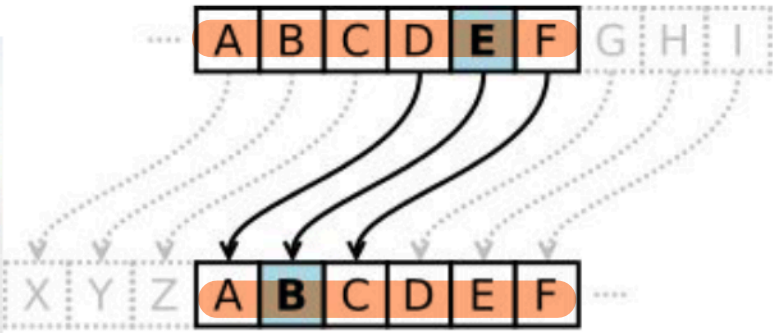


UNIVERSITÀ DEGLI STUDI DI PADOVA

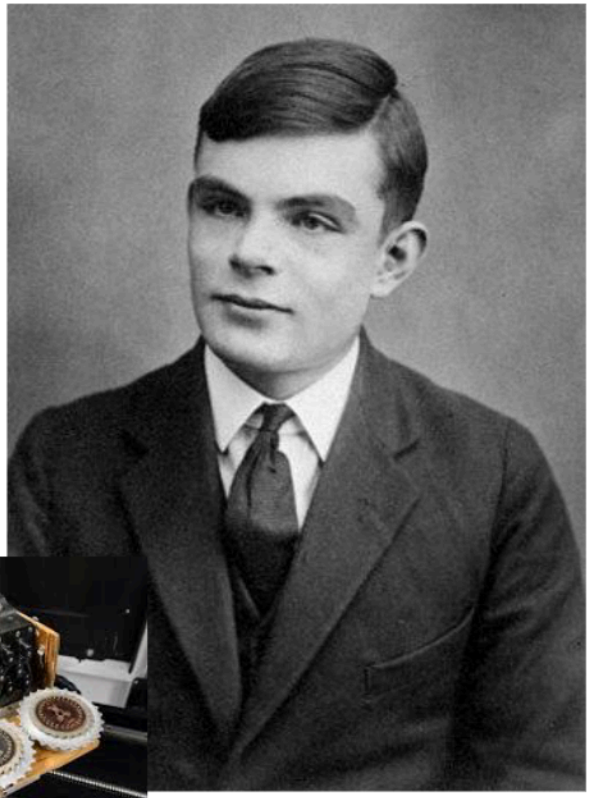
SPRITZ SECURITY & PRIVACY RESEARCH GROUP

DIPARTIMENTO MATEMATICA

Historical Facts

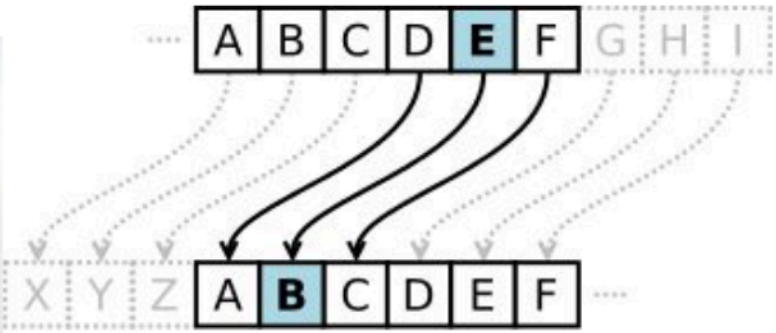


Ceasar Cipher: private correspondence (~50BC)

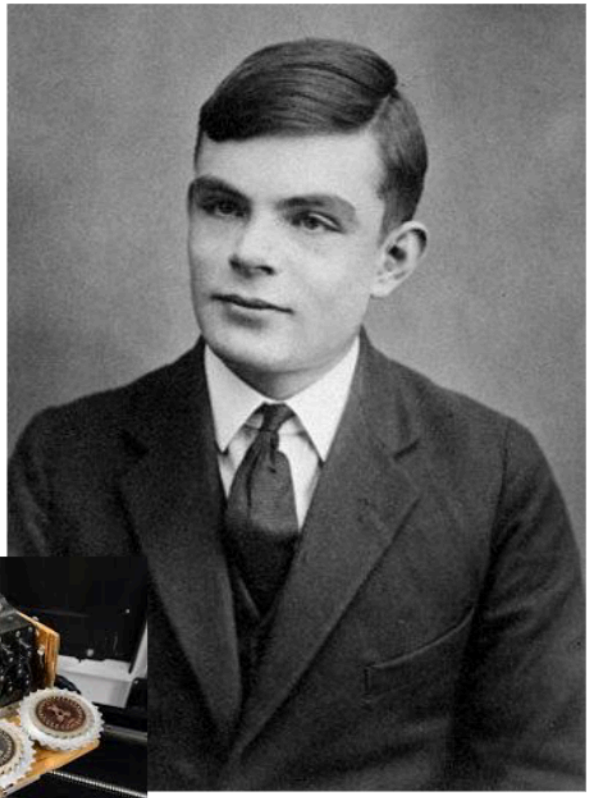


Alan Turing: decryption of German's ciphers during WWII (1940s)

Historical Facts



Ceasar Cipher: private correspondence (~50BC)



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

Introduction

- 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

Encryption

Insecure channel

Encryption

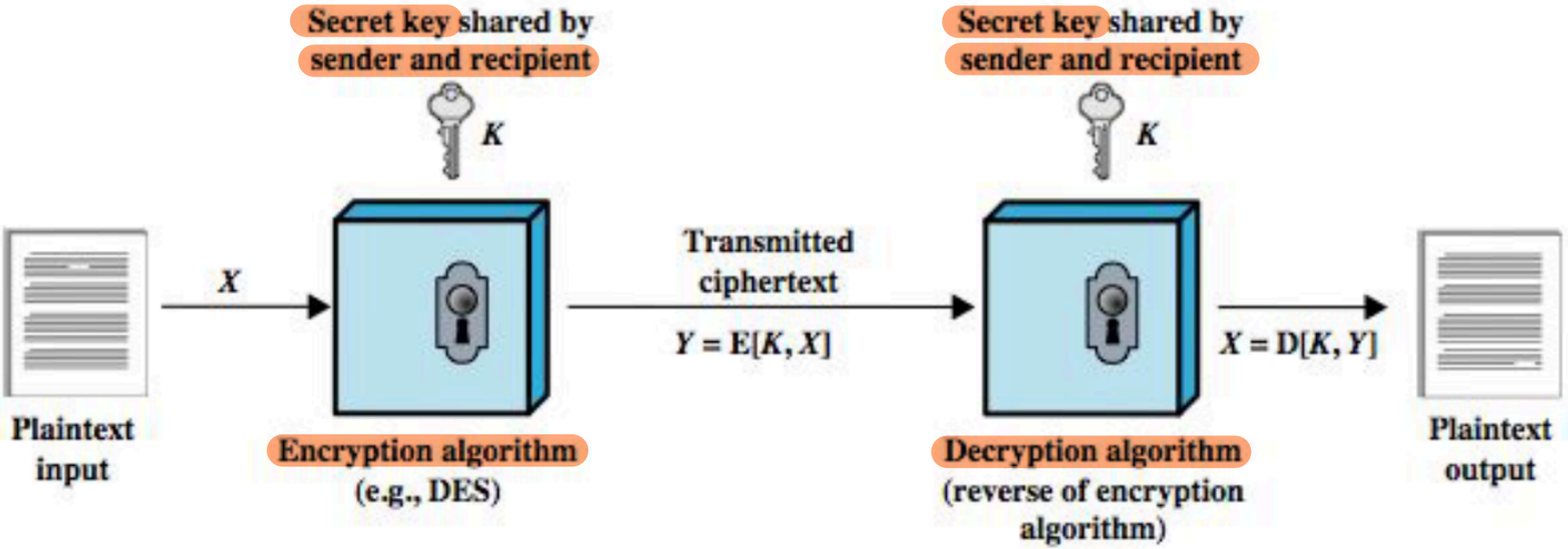
Alice (sender)

Insecure channel

Bob (receiver)

Eve (adversery)

Symmetric Encryption



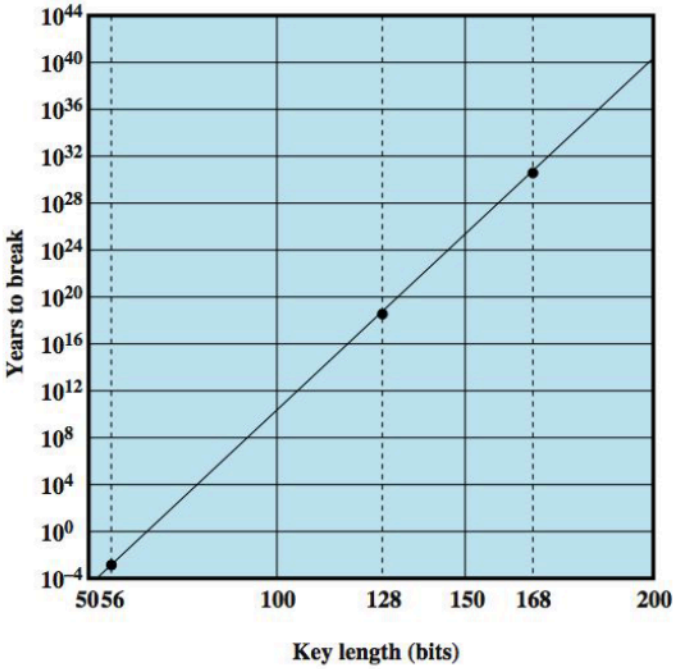
Symmetric Encryption - Threats

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



Symmetric Encryption

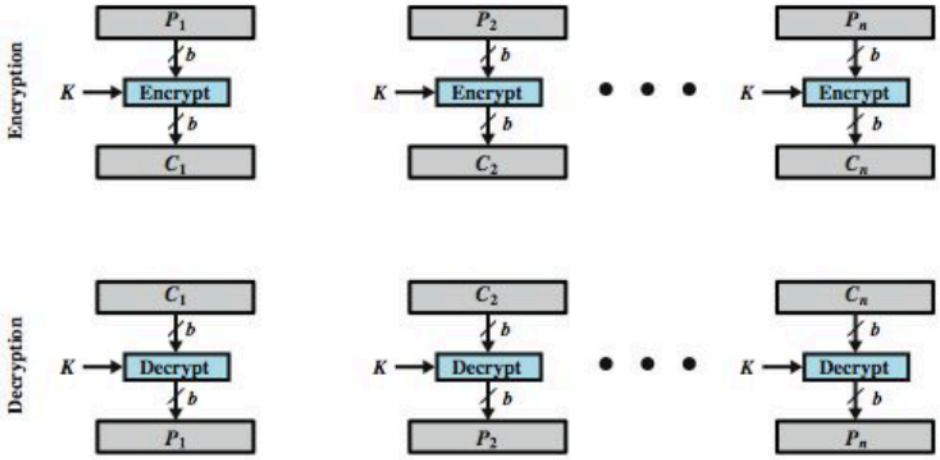
	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

DES and Triple-DES

- 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



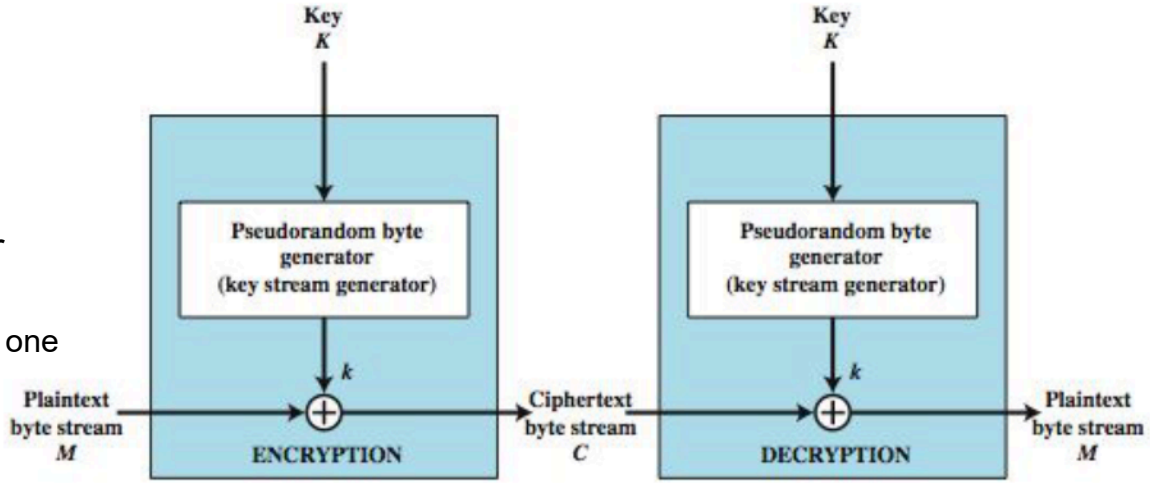
(a) Block cipher encryption (electronic codebook mod

Encryption on Blocks (DES)

- A key per a single block

Encryption on single Character

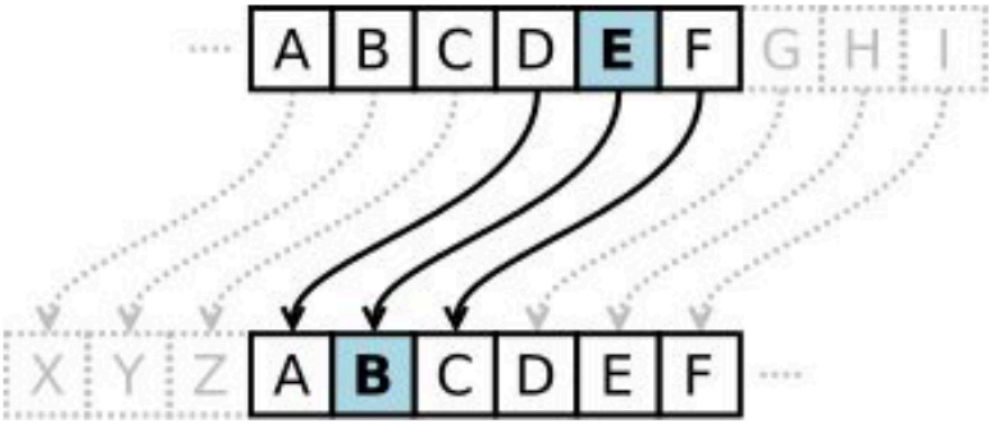
- Same key for every character of different one



(b) Stream encryption

Example 1 - Caesar Cipher

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



When cipher is additive, the plain text, the cyphred text, and the key are in 0<c<26

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”

Cryptographic Tools: XOR

- XOR is it widely adopted in crypto algorithms
  - Boolean operation
    - 0 xor 0 = 0
    - 0 xor 1 = 1
    - 1 xor 0 = 1
    - 1 xor 1 = 0
  - Represented with the symbol " ^ "
- enc_message = clear_message ^ key

Only one 1 is necessary for 1

Cryptographic Tools: XOR

Properties:

- XOR is commutative
  a ^ b = b ^ a
- XOR is associative
  a ^ (b ^ c) = (a ^ b) ^ c
- Anything XORed with itself is zero
  a ^ a = 0
- Anything XORed with zero is anything
  a ^ 0 = a

Cryptographic Tools: XOR

enc_message = clear_message ^ key

clear_message = enc_message ^ key

key = clear_message ^ enc_message

Cryptographic Tools: XOR

- XOR is used between a key and a message
  - Often len(key) << len(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.

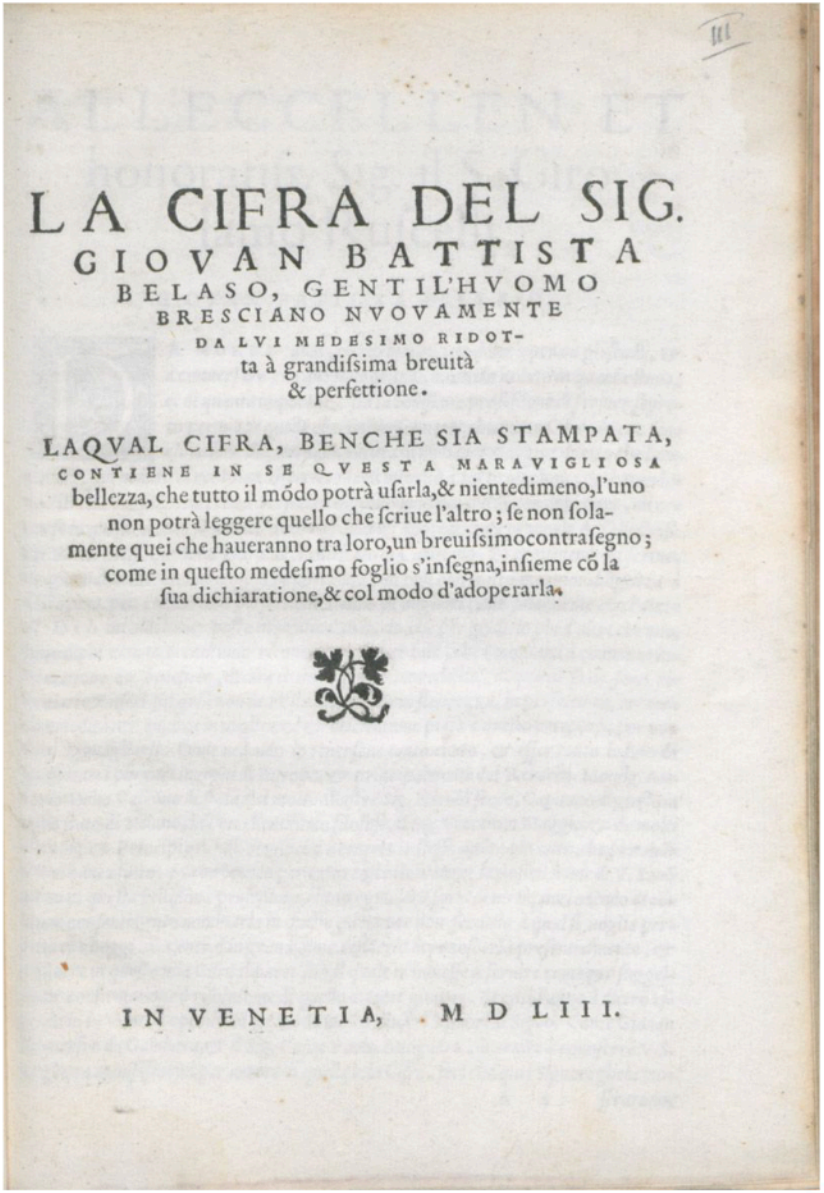
- 84 = 1010100
- 89 = 1011001
- 13 = 0001101

XOR - Kasiski Elimination

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

XOR - Kasiski Elimination



LA CIFRA DEL SIG.
GIOVAN BATTISTA
BELASO, GENTIL'HVOMO
BRESCIANO NVOVAMENTE
DA LVI MEDESIMO RIDOT-
ta à grandiſsima breuità
& perfettione.

LAQVAL CIFRA, BENCHE SIA STAMPATA,
CONTIENE IN SE QVESTA MARAVIGLIOSA
bellezza, che tutto il mõdo potrà uſarla,& nientedimeno,l'uno
non potrà leggere quello che ſcriue l'altro; ſe non ſola-
mente quei che haueranno tra loro,un breuiſsimocontraſegno;
come in queſto medeſimo foglio s'inſegna,inſieme cõ la
ſua dichiaratione,& col modo d'adoperarla.

IN VENETIA, M D LIII.

Student @ UniPD ~1537

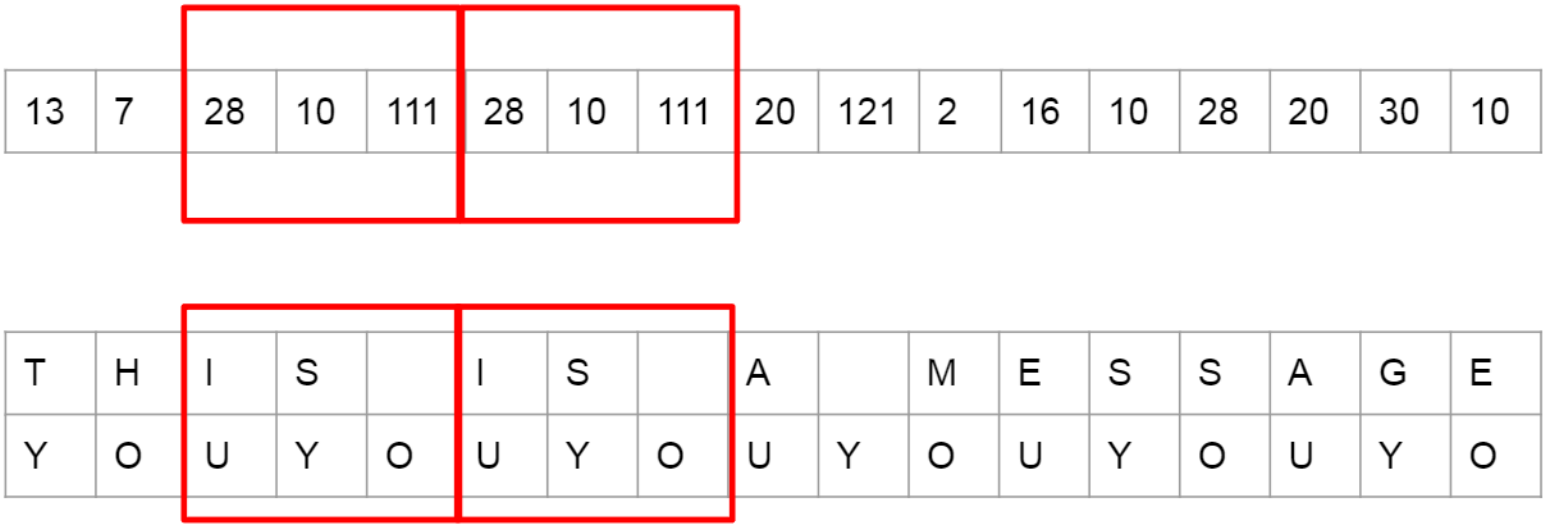
ISTITUTO
PER LA STORIA DELL'UNIVERSITÀ DI PADOVA

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?