HOGWORDS
School of Cryptography for Young Learners
Erasmus+
31 May 2022 - 31 May 2024

Hogwords

School of Cryptography for Young Learners

Lessons Calendar

Thursday h 18-20

12th October 2023 – 18th April 2024

PART 1 - TOOLS

1. Arithmethic

12 OTTOBRE h 18-20 Warm-up: Primes, Divisibility and the Fundamental Theorem of Arithmetic.

26 OTTOBRE Greatest Common Divisor (GCD), Euclidean Algorithm, Bézout identity.

9 NOVEMBRE H 18-20 Modular Arithmetic and congruences: Fermat's little Theorem, Eulero's phi function and Chinese Remainder Theorem.

23 NOVEMBRE H 18-20 Mathematics of R.S.A.

2. Coding

7 DICEMBRE H 18-20 problem - algorithm - program
programming languages
interpretation, executable program
working environments, syntactic errors, debugging
expression, variable, assignment, function call
help
types

21 DICEMBRE H 18-20 input/output
if ... else ...
working with lists, strings

defining functions
recursion (overview)
cycles
simple problems on lists

11 GENNAIO H 18-20 search in a list: sequential, binary search
numeric algorithms: zero of a continuous function
GCD (greatest common divider)
evaluating a polynomial (Horner)
russian peasant multiplication algorithm

25 GENNAIO H 18-20 dictionaries
computing frequencies,
working with text files

8 FEBBRAIO H18-20 more problems ...

PART 2 - Cryptography

22 FEBBRAIO H 18-20 Information security (infosec) and its requirements
Standards for infosec
Threats and attacks

7 MARZO H 18-20 Encryption model
Symmetric encryption
Mono-alphabetic substitution
Attack based on frequency analysis
Modern ciphers and AES
ECB and CBC

21 MARZO H 18-20 Data integrity
Cryptographic hashing and collisions
Birthday paradox and attack
Keyed and unkeyed hashing
HMAC

4 APRILE H 18-20 Public key cryptography
Textbook RSA
Key generation

Public and private key and relationship between them
Digital certificates
Example through openssl

18 APRILE H 18-20 Digital signature and non-repudiation
CAdES/PAdES
Verification
Common errors
SW for signing/verifying
Public key cryptography for authentication and passkeys

Final week – Cryptography contest and orientation activities

From the 6th to the 10th of May 2024
CNR – IAC Rome, via dei Taurini 19
Sapienza University Rome, Piazzale Aldo Moro 1
Details will be given later