UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Teoria dell'Informazione e Crittografia

2526-1-F1802Q139

Aims

Knowledge and understanding
Students will understand the operating principles of error correction codes, and some simple lossless data compression techniques (that is, without loss of information). They will also understand how a cryptosystem or cryptographic protocol works.

Applied knowledge and understanding
Students will be able to choose the appropriate cryptographic tools to protect data during transmission and/or storage.

Independent judgment
Students will acquire the ability to evaluate whether the proposed error correction, data compression, and encryption algorithms are adequate.

Communication skills
The great attention paid to formal aspects will allow students to understand the importance of unambiguous communication, using the correct terminology to express the notions and concepts learned.

Learning skills
The formalization of concepts will facilitate deductive learning mechanisms. Furthermore, presenting examples and exercises on the board, immediately after explaining a technique or algorithm, helps clarify any doubts and particular cases.

Contents

Basic notions and concepts of Information Theory, Coding Theory, and modern Cryptography. The course also

provides the conceptual and theoretical tools that allow the student to understand the advanced techniques which are currently used to protect data transmission and storage, in presence of malicious adversaries or noise in the communication channel.

Detailed program

1. Error-correcting codes:

- Definitions of source, channel, and encoding
- Error-detecting codes. Parity checks
- Error-correcting codes. Geometric and algebraic approaches. Hamming codes

2. Source encoding:

- Prefix-free codes and their construction
- Kraft and McMillan inequalities
- Huffman codes

3. Entropy:

- Definition and mathematical properties
- Shannon-Fano codes
- Shannon's noiseless coding theorem

4. The noisy channel:

- Definition of channel, associated entropies and mutual information
- Channel capacity
- The binary symmetric channel
- Shannon's main theorem

5. Introduction to Cryptography:

- Definition of cryptosystems
- Attack models
- Historical cryptosystems, and their analysis

6. Symmetric cryptosystems:

- Standard cryptosystems: DES, 3DES and AES
- Modes of operation of symmetric cryptosystems

7. Theoretical foundations of symmetric cryptosystems:

- Confusion and diffusion
- Permutation-substitution networks
- Feistel’s structure

8. Public-key cryptosystems:

- One-way functions: discrete logarithms and factorization
- Diffie-Hellman's protocol. The ElGamal cryptosystem. Hybrid cryptosystems

- The RSA cryptosystem. Some simple attacks to RSA. Randomized RSA

9. Pseudorandom number generators
10. Digital signature schemes
11. Cryptographic hash functions
12. Introduction to post-quantum cryptography

Prerequisites

Topics explained in mathematics courses held in the laurea degree in Informatics. It is useful - but not necessary - to have basic notions of theoretical computer science (in particular, Turing machines).

Teaching form

20 lessons of 2 hours held in the classroom, in delivery mode, in presence.
10 exercises of 2 hours held in the classroom, in delivery mode, in presence.

The expected teaching language is Italian. However, lectures and exercises may be provided in English if at least one of the following conditions is met:

- in the classroom there is at least one foreign student who does not speak Italian;
- the students request to attend lectures and exercises given in English.

All lectures and exercises made in the classroom will be recorded, and made available inside the Web page of the course.

Textbook and teaching resource

Textbooks:

- R.W. Hamming. Coding and Information Theory. Second edition, Prentice-Hall, 1986
- D.R. Stinson. Cryptography: Theory and Practice. Fourth Edition, CRC Press, 2018

Lecture notes provided by the teacher.

Semester

Second semester

Assessment method

The learning assessment is based on an oral interview, on the subjects exposed in class during the course. During the interview, the student's ability to explain the topics of the course, and to make brief thoughts on them, will be assessed.

There are no mid-term evaluations.

Office hours

On appointment

Sustainable Development Goals

QUALITY EDUCATION