UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

COURSE SYLLABUS

Information Theory and Cryptography

2425-1-F1801Q122

Aims

Understanding of the principles of operation of error-correcting codes, and of some simple techniques for lossless data compression. Ability to understand the functioning of cryptosystems and cryptographic protocols. Ability to choose the most suitable cryptographic tools to protect data during their transmission and/or storage.

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

3. Source encoding:

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

- Huffman codes

5. Entropy:

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

7. The noisy channel:

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

9. Introduction to Cryptography:

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

11. Symmetric cryptosystems:

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

13. Theoretical foundations of symmetric cryptosystems:

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

15. 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

17. Pseudorandom number generators
18. Digital signature schemes
19. Cryptographic hash functions

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

Classrom lectures and exercises, held in delivered mode, in person.

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, Academic Year 2024-2025

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 ongoing tests.

Office hours

On appointment

Sustainable Development Goals

QUALITY EDUCATION