

COM-102

Advanced information, computation, communication II

Gastpar Michael

Cursus	Sem.	Type
Communication systems	BA2	Obl.
Computer science	BA2	Obl.

Language of teaching	English
Coefficient	7
Session	Summer
Semester	Spring
Exam	Written
Workload	210h
Weeks	14
Hours	6 weekly
Courses	4 weekly
Exercises	2 weekly
Number of positions	

Summary

Text, sound, and images are examples of information sources stored in our computers and/or communicated over the Internet. How do we measure, compress, and protect the information they contain?

Content

I. How to measure information. Source modeling and probability. Entropy. Source coding and compression. Entropy to analyze algorithms.

II. Cryptography and information security. Modular arithmetic, modern algebra and number theory. The Chinese remainder theorem and RSA.

III. Protecting information. Channel modeling. A few finite fields. Vector spaces. Hamming distance. Linear codes. Reed-Solomon codes.

Keywords

Entropy
 Data compression
 Number theory
 Cryptography
 RSA cryptosystem
 Linear codes
 Reed-Solomon codes

Learning Outcomes

By the end of the course, the student must be able to:

- Understand Shannon's entropy
- Construct an optimal code
- Understand elementary number theory
- Know what an abelian group is
- Recognize a hidden isomorphism
- Know how RSA works
- Know a few linear codes on simple finite fields

Transversal skills

- Take feedback (critique) and respond in an appropriate manner.
- Assess one's own level of skill acquisition, and plan their on-going learning goals.

Teaching methods

Ex cathedra with exercises

Expected student activities

Homework (written and grades) ever week.

Assessment methods

Continuous evaluations 10% and final exam 90%

Resources

Bibliography

"Sciences de l'information", J.-Y. Le Boudec, R. Urbanke et P. Thiran, online

Ressources en bibliothèque

- [Find the references at the Library](#)

Moodle Link

- <https://go.epfl.ch/COM-102>