Advanced information, computation, communication II

Rimoldi Bixio

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 and probability. Entropy per symbol. Source coding.

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


Keywords
Shannon's entropy
Linear codes
Reed-Solomon codes
Number theory
Asymmetric Cryptography, RSA

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) every 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

• Introduction aux sciences de l'information : entropie, compression, chiffrement et correction d'erreurs / Le Boudec

Moodle Link

• http://moodle.epfl.ch/course/view.php?id=851