Introduction to cryptography

M1, 2014-2015

Computer Science Department, ENS de Lyon

Lecturers: Benoît Libert and Damien Stehlé
Teaching assistant: Vincent Neiger

Cryptography aims at securing communications against malicious parties. This field enjoys numerous links with theoretical computer science (complexity theory, security proofs) but has also a very rich practical counterpart: Cryptographic protocols are part of everyday life (electronic commerce, payment cards, electronic voting, etc). This course is an introduction to the different facets of modern cryptography. The following topics will be addressed: symmetric encryption, asymmetric encryption, cryptographic hashing, authentication, pseudo-random number generators, zero-knowledge proofs, public-key infrastructure, cryptanalysis, secret sharing.

Course objectives

1. Understand the different basic primitives (PRNG, PRF, encryption, MAC, hash function, key exchange, digital signature).
2. Understand the different attack scenarios.
3. Be able to devise a security proof, in the standard model and in the random oracle model.
4. Understand the hardness assumptions used in asymmetric cryptography (factoring, RSA problem, discrete logarithm, decision Diffie-Hellman).
5. Be able to use elementary number theory to study asymmetric primitives.

Evaluation

Final exam (counts two thirds of the final mark): 3 hours, written notes allowed.

Continuous assessment (counts one third of the final mark): partial exam, one or two homework assignements, randomly selected-corrected-graded tutorials.