Computer Algebra and cryptography

2 courses

One in common with « M1-Maths-Générales »
One specific to M1-MSIAM

About the first course

Objective : Mathematical fondations and theory for cryptography

Format: 9 Lectures, and experimentations on mathematical software.

-Modular arithmetic
-Ideas of complexity (what is easy to compute, what is hard to compute)
-Finite fields and error correcting codes
-Pseudo-random generators
-Asymmetric technics, Diffie-Hellman keys, El Gamal and RSA encryption
-Attacks on discrete logarithm, and integer factorisation
-Primality tests

Computer Algebra and cryptography

2 courses

One in common with « M1-Maths-Générales »
One specific to M1-MSIAM

About the second course

Objective : Presentation of symmetric cryptography and some practical aspects of using cryptography in general
Format: Mix of lectures, exercices and lab sessions (likely in C)

- Definition of security properties, modeling of adversaries
- Construction of block ciphers, hash functions, MACs, modes of operation
- How to properly use RSA, how to choose a Diffie-Hellman group
- Presentation of password-hashing techniques
- Examples of attacks and tradeoffs (e.g. based on finding collisions)
- Introduction to implementation aspects of cryptographic algorithms