UE Advanced cryptology

Level
Baccalaureate +5

ECTS
6 credits

Component
UFR IM2AG (informatique, mathématiques et mathématiques appliquées)

Semester
Automne

- **Teaching language(s):** English
- **Teaching method:** In person
- **Teaching type:** Lectures
- **Open to exchange students:** Yes
- **Code d'export Apogée:** GBX9SY07

Presentation

Description

The aim of this course is to present some advanced topics in cryptography. The exact content may vary from one year to another; as an indication past topics have included:
- Linear secret sharing schemes (code-based schemes, access structures...)
- Provable constructions in symmetric cryptography (building block cipher from ideal permutations)
- Symmetric cryptanalysis (statistical and algebraic)
- Algorithms and constructions in code-based cryptography (information-set decoding, LPN)
- Zero-knowledge proofs
- Advanced signatures (group signatures...)
- Advanced constructions (oblivious transfer, group encryption...)
- Post-quantum cryptography
- Elliptic-curve and isogeny-based cryptography

Course parts

TP	Practical work (TP)	12h
CM	Lectures (CM)	24h
TD	Tutorials (TD)	12h

Recommended prerequisites

A good knowledge of basic notions in cryptography (security definitions, classical constructions...) is expected. This should also be complemented by good skills in algorithmics and discrete mathematics (finite fields, linear algebra, statistics, elementary algebraic geometry...).

Period : Semester 9

Useful info

Contacts

Program director

Pierre Karpman

pierre.karpman@univ-grenoble-alpes.fr

Program director

Emmanuel PEYRE

Place

Grenoble

Campus

Grenoble - University campus