UE Advanced Cryptology

Niveau d'étude
Bac +5

ECTS
6 crédits

Crédits ECTS Echange
6.0

Composante
UFR IM2AG (informatique, mathématiques et mathématiques appliquées)

Période de l'année
Automne (sept. à dec./janv.)

- **Langue(s) d'enseignement:** Anglais
- **Méthodes d'enseignement:** En présence
- **Ouvert aux étudiants en échange:** Oui
- **Crédits ECTS Echange:** 6.0
- **Code d'export Apogée:** GBX9SY07

Présentation

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

Informations non contractuelles.
Dernière mise à jour le 10 juillet 2024

Heures d'enseignement

CM	CM	24h
TD	TD	12h
TP	TP	12h

Pré-requis recommandés

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...).

Période : Semestre 9

Infos pratiques

Contacts

Responsables pédagogiques

Pierre Karpman

pierre.karpman@univ-grenoble-alpes.fr

Responsables pédagogiques

Emmanuel PEYRE

Campus

Grenoble - Domaine universitaire

Informations non contractuelles.
Dernière mise à jour le 10 juillet 2024