

UE Cryptographic engineering, protocols and security models, data privacy, coding and applications



Niveau d'étude
Bac +5



ECTS
6 crédits



Crédits ECTS
Echange
6.0



Composante
UFR
Informatique,
mathématiques
et
mathématiques
appliquées
(IM2AG)



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

Diplômes intégrant cet élément

- Master Informatique

- › **Langue(s) d'enseignement:** Anglais
- › **Méthodes d'enseignement:** En présence
- › **Forme d'enseignement :** Cours magistral
- › **Ouvert aux étudiants en échange:** Oui
- › **Crédits ECTS Echange:** 6.0
- › **Code d'export Apogée:** GBX9SY03

Présentation

Description

The course present the main cryptographic primitives and security protocols, focusing on security parameters and properties.

Pedagogical goals:

- generic cryptographic primitives: one-way, trap-door and hash functions; random generators; symmetric and assymertic cipher; interactive protocols;

- security properties : complexity and reduction proofs; undistinguishability; non-malleability; soundness, completeness and zero-knowledge; confidentiality; authentication; privacy; non-repudiation
- use, deployment and integration of protocols in standard crypto lib (eg openssl)
- security proofs : foundations and verification based on tools (eg avispa)

Heures d'enseignement

CM	CM	36h
TD	TD	18h
TP	TP	24h

Période : Semestre 9

Infos pratiques

Contacts

Responsable d'UE

Clement Pernet

✉ Clement.Pernet@univ-grenoble-alpes.fr

Lieu(x) ville

➤ Grenoble

Campus

➤ Grenoble - Domaine universitaire