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

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:** GBX9SY03

Presentation

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; undistinguidhability; non-malleability; soundness, completeness and zero-knowledge; confidentiality; authentication; privacy; non-repudiation

- use, deployment and integration of protocols in standard crypro lib (eg open-ssl)

- security proofs : fundations and verufucation based on tools (eg avispa)

Course parts

TP	Practical work (TP)	24h
TD	Tutorials (TD)	18h
CM	Lectures (CM)	36h

Period : Semester 9

Useful info

Contacts

Program director

Clement Pernet

Clement.Pernet@univ-grenoble-alpes.fr

Place

Grenoble

Campus

Grenoble - University campus