Digital educational booklet 2017/2018

Advanced cryptography (E-Secure)

3IMR3	**Advanced cryptography (E-Secure)**	**Computer Science**	**S9**

Cours : 20 h	**TD : 0 h**	**TP : 0 h**	**Projet : 0 h**	**Total : 20 h**

Responsable : Regis Clouard

Pré-requis

Mathematics for computer science
Cryptography

Objectifs de l'enseignement

The aim is to give advanced knowledge in cryptography with non-trivial notions of the domain.

Programme détaillé

This course covers the notions of security models, generic constructions of secure encryption, provable security, authentication (symmetric and asymmetric MAC, signature, proof of identification and security), interactive and non-interactive zero-knowledge protocols, the key distribution, secret sharing, distributed computing course. This course will also address more complex systems like electronic voting or e-cash protocols based on "special" signatures. This course will also address the so-called "post-quantum" cryptography (supposed to resist the advent of quantum computers), as well as pairing based cryptography defined on elliptic curves.

Applications (TD ou TP)

e-voting, e-cash, privacy, e-payment, ...

Compétences acquises

Advanced knowledge in cryptography and sécurity

Bibliographie

Non renseigné