

Présentation

Code interne : EIN8-SECU1

Description

Après quelques rudiments en Théorie des Nombres et en Théorie de la Complexité, ce cours d'initiation présente une grande variété de protocoles et étudie la sécurité de certains d'entre eux.

Plan

Introduction aux protocoles - Introduction - Cryptosystèmes à clefs secrètes

Sécurité des protocoles - De la difficulté en Théorie de la Complexité - Systèmes à clefs publiques - Quelques problèmes arithmétiques faciles - Quelques problèmes arithmétiques difficiles

Exemples de protocoles - Protocole de mise en gage - Signature et authentification - Preuve à divulgation nulle - Paiement et vote électronique

Perspectives - Cryptologie quantique

Heures d'enseignement

CI	Cours Intégrés	24h
TD	Travaux Dirigés	6h
TI	Travaux Individuels	20h

Pré-requis obligatoires

[[m:IF101]], [[m:IF102]], [[m:IF106]]

Syllabus

- I. Introduction aux protocoles
 - Introduction

- Cryptosystèmes à clefs secrètes
- II. Sécurité des protocoles
- De la difficulté en Théorie de la Complexité
 - Systèmes à clefs publiques
 - Quelques problèmes arithmétiques faciles
 - Quelques problèmes arithmétiques difficiles
- III. Exemples de protocoles
- Protocole de mise en gage
 - Signature et authentification
 - Preuve à divulgation nulle
 - Paiement et vote électronique
- IV. Perspectives
- Cryptologie quantique

Modalités de contrôle des connaissances

Évaluation initiale / Session principale

Type d'évaluation	Nature de l'évaluation	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'évaluation	Note éliminatoire de l'évaluation	Remarques
Contrôle Continu Intégral	Contrôle Continu			1		

Infos pratiques

Contacts

Responsable module

Mihail Popov

✉ Mihail.Popov@bordeaux-inp.fr