

↳ **Tour de contrôle des U.E**  
*(Une fiche par semestre et par UE)*

## Licence Sciences et Technologies

Libellé long: Introduction à la cryptographie

Libellé court: Intro. à la cryptographie

Composante: U.F.R. Sciences

Période: Enseignement premier semestre

Nature: Unité d'enseignement

Crédit ECTS: 2

Volume: 18 HE

### Objectifs

Découverte et mise en oeuvre des principes de bases de la cryptographie moderne.

### Programme contenu

Ce cours commence par relater l'histoire de la cryptologie, avant qu'elle ne devienne la discipline scientifique de pointe qu'elle est aujourd'hui, entre informatique et mathématiques. Le cours présente des méthodes de chiffrement à clé secrète (DES, AES) et des méthodes de chiffrement à clé publique (protocole de Diffie-Hellman, RSA). On ne fera qu'évoquer les dernières avancées dans le domaine.

La cryptographie ne se limite pas au chiffrement des messages, d'autres notions seront présentées comme la signature, l'identification, l'authentification, l'intégrité des données, les certificats. On recensera aussi les usages quotidiens de la cryptographie: connexion à un système informatique, commerce électronique, carte bleue, envoi de données sécurisé, one-time password...

Enfin, on analysera les évolutions qu'a entraîné la cryptographie moderne (lois, autorités de certification, e-commerce, autorités de certification, etc).

Les TP mettront en oeuvre les protocoles classiques de chiffrement ou de signature. Ils permettront aussi de fouiller les applications informatiques pour comprendre où s'y loge la cryptographie.

## Charges

C.N.U: Informatique

Cours magistraux: 9 heures

Travaux dirigés: 0 heures

Travaux pratiques: 9 heures

## Responsables

- FORMENTI Enrico

## Ressources BU ou ouvrages conseillées

Codage, cryptologie et applications

Bruno Martin. Presses Universitaires Romandes, 2004.

## Ressources numériques

<http://fr.wikipedia.org/wiki/Cryptologie>

<http://deptinfo.unice.fr/LST-I/DescriptifUE/Crypto>