Mathématiques pour l'informatique (INFO602_INFO)

Composante
UFR Sciences
et Montagne

En bref

- **Langues d'enseignement:** Français
- **Méthodes d'enseignement:** En présence
- **Ouvert aux étudiants en échange:** Oui

Présentation

Description

Démystifier certaines applications des mathématiques pour l'informatique, utilisation de ces techniques et étude de quelques exemples (codes correcteurs d'erreurs, aléatoire, cryptographie)

Les TP se feront en utilisant le langage C et permettront d'approfondir les exemples vus en cours et TD : implémentation d'un système de détection et correction d'erreurs, inversion (« craquage ») de générateurs aléatoires simples, implémentation de l'attaque FMS sur le chiffrement WEP.

Heures d'enseignement

CM	Cours Magistral	6h
TD	Travaux Dirigés	9h
TP	Travaux Pratiques	12h

Plan du cours

- codes correcteurs d'erreurs, matrices génératrice / matrices de parité, applications et exemples ;

- générateurs aléatoires : congruences linéaires et systèmes à rétroaction, propriétés et applications, utilisation des générateurs aléatoires ;

- cryptographie : historique et concepts fondamentaux, cryptographie symétrique, systèmes de chiffrement par blocs et leurs modes de fonctionnement, rappels d'arithmétique modulaire et cryptographie asymétrique.

Libellé court : INFO602_INFO

Nature : MODL

Infos pratiques

Lieux

Le Bourget-du-Lac (73)

Campus

Le Bourget-du-Lac / campus Savoie Technolac

Contacts

Responsable du cours

Francois Boussion