Master Mathématiques et applications
Fondements mathématiques de la cryptographie

Responsable

Joaquin RODRIGUES JACINTO
joaquin.RODRIGUES-JACINTO@univ-amu.fr

Descriptions

Code : SMACK3A

Nature :

Domaines : Sciences et Technologies

Informations

Composante : Faculté des Sciences

Nombre de crédits :

LANGUE(S) D'ENSEIGNEMENT

Français

CONTENU

Le but de ce cours est de fournir les outils mathématiques nécessaires pour comprendre les bases de la cryptographie moderne ainsi que pour étudier et implémenter les cryptosystèmes classiques.

Contenus :

- Arithmétique modulaire, symbole de Legendre et Jacobi, tests de primalité (Rabin-Miller, Baillie–PSW), logarithme discret.
- Cryptographie symétrique et asymétrique. Échange de clés de Diffie-Hellman, cryptosystème ElGamal, RSA.
- Cryptanalyse : Baby Step Giant Step, algorithme rho Pollard, algorithme de factorisation de Pollard.
- Sujets avancés : Cryptographie sur les courbes elliptiques, cryptographie sur les réseaux, codes correcteurs d'erreurs.

VOLUME HORAIRE

- Volume total: 18 heures
- Cours magistraux: 11 heures
- Travaux dirigés: 7 heures

CODES APOGÉE

- SMACK3AL [ELP]

M3C

Aucune donnée M3C trouvée

POUR PLUS D'INFORMATIONS

Aller sur le site de l'offre de formation...

Dernière modification le 15/07/2024