Master Informatique
Cryptographie

Dernière modification le 13/11/2024

Informations

Composante : Faculté des Sciences

Responsable

Remi MORIN

Langue(s) d'enseignement

Français

Contenu

Cette ECUE présente un tour d'horizon de la cryptographie moderne en suivant les trois problématiques classiques du domaine : confidentialité, authentification et intégrité.

Plan:

1. Introduction aux concepts cryptographiques
2. Chiffrement symétrique par flot et par bloc (AES)
3. Arithmétique et algorithmique & protocole RSA
4. API JCE - Trousseau
5. Chiffrements asymétriques, signatures et certificats
6. Logarithme discret - Echanges de clefs

Compétences à acquérir

- Connaître et savoir reconnaître une problématique cryptographique
- Connaître et savoir mettre en oeuvre dans une application les solutions recommandées
- Comprendre l'importance du choix des paramètres recommandés par l'ANSSI

Modalités d'organisation

Cours magistraux (CM) et Travaux Pratiques (TP)

Bibliographie, lectures recommandées

GUIDE DE SÉLECTION D'ALGORITHMES CRYPTOGRAPHIQUES, ANSSI, 2021.

Pré-requis obligatoires

Programmation en Java

Prérequis recommandés

Unix

VOLUME HORAIRE

- Volume total: 27 heures
- Cours magistraux: 9 heures
- Travaux dirigés: 9 heures
- Travaux pratiques: 9 heures

Codes Apogée

- SINA09FL [ELP]

Pour plus d'informations

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