



Sécurité Numérique Matérielle



Présentation

Description

- Objectifs et enjeux de de la sécurité matérielle
- Chiffrement symétrique (DES, AES) et architectures microélectroniques associées
- Calcul modulaire et multiplication des grands nombres
- Chiffrement asymétrique (RSA) et architectures microélectroniques associées
- Principe d'Authentification
- Génération de nombres aléatoires
- Attaques par canaux cachés
- Attaques en fautes

Objectifs

Acquérir les bases pour la compréhension des notions de cryptographie et d'attaques sur les systèmes matériels implantant ces algorithmes.

Pré-requis obligatoires

Électronique digitale

Pré-requis recommandés* :



Programmation et langage de description matérielle

Syllabus

Livre : "Handbook of Applied Cryptography" - <http://cacr.uwaterloo.ca/hac/>

Informations complémentaires

CM : 13h30

TP : 3h

Infos pratiques

Contacts

Responsable pédagogique

Arnaud VIRAZEL

✉ Arnaud.Virazel@umontpellier.fr