

# SECURITE NUMERIQUE

## **Objectif - Compétences acquises :**

Avoir une première expérience en sécurité numérique • Comprendre les enjeux de la sécurité matérielle • Expliquer les principaux algorithmes cryptographiques • Comprendre les vulnérabilités potentielles de ces algorithmes • Pratiquer des attaques par canaux cachés

### **Public concerné :**

- Industriel

### **Durée :**

- 2 jours

### **Date/lieux :**

- Nous consulter
- Non défini

### **Equipe pédagogique :**

- Enseignants-chercheurs de l'Université de Montpellier

### **Approche pédagogique :**

- Alternance de cours, de TD et de travaux pratiques

### **Renseignement pédagogique :**

- Bruguier Florent
- secnum@cnfm.fr

### **Frais de participation individuels :**

- 800 € HT

### **Renseignements et inscriptions :**

- Inscription : Service de Formation Continue de l'Université de Montpellier
- Tél : +33(0) 6 82 92 28 27
- Fax : +33(0) 4 34 43 21 90
- Email : catherine.bellanger@umontpellier.fr
- Date limite d'inscription : 1 mois avant

### **Nombre de places limitées :**

- Min/Max : 3 à 8 personnes

### **Prérequis :**

- Une connaissance des bases de l'électronique et des systèmes numériques est nécessaire pour cette formation.

### **Programme :**

- Introduction à la cryptographie et la cryptanalyse : Terminologie et définitions
- Enjeux de la sécurité numérique
- Les algorithmes de chiffrement symétriques (DES, AES ....)
- Les algorithmes de chiffrement asymétriques (RSA, ECC..)
- Principe des attaques par canaux cachés • Présentation de la Plateforme SECNUM
- Etude de l'implantation matérielle de l'AES sur FPGA
- Mise en place d'une attaque et instrumentation
- Campagne d'acquisition et analyse des résultats
- Principe des attaques différentielles et corrélatives
- Etude de différents modèles de prédiction
- Mise en œuvre d'une attaque
- Optimisation des attaques
- Principes des contre-mesures

### **Validation :**

Cette formation constitue une action d'adaptation et de développement des compétences. Elle donne lieu à la délivrance d'une attestation de participation. Une évaluation de fin de formation permet de mesurer la satisfaction des stagiaires, notamment concernant l'atteinte des objectifs pédagogiques.