


# UE Introduction to cryptology

 ECTS  
3 crédits

 Composante  
UFR IM2AG  
(informatique,  
mathématiques  
et  
mathématiques  
appliquées)

- > **Langue(s) d'enseignement:** Français
- > **Méthodes d'enseignement:** En présence
- > **Forme d'enseignement :** Cours magistral
- > **Ouvert aux étudiants en échange:** Non

## Présentation

### Description

Cette UE est une exposition des fondements mathématiques de certains protocoles et de certaines méthodes utiles en cryptologie moderne.

- 1- Arithmétique modulaire, et applications
- 2- Codes correcteurs d'erreurs
- 3- Suites récurrentes linéaires, registres à décalage, et corrélations
- 4- Protocoles asymétriques, Diffie Hellman ; El Gamal ; RSA
- 5- Sécurité et attaques
- 6- Trouver des nombres premiers, tests de primalité.

Au cours des thèmes abordés, on expérimentera en TP certaines notions avec des outils de calcul formel.

---

## Heures d'enseignement

UE Introduction to cryptology - CM	CM	15h
UE Introduction to cryptology - TD	TD	9h
UE Introduction to cryptology - TP	TP	9h

**Période** : Semestre 8

## Infos pratiques

---

### Contacts

Responsable pédagogique

Francois Dahmani

✉ [Francois.Dahmani@univ-grenoble-alpes.fr](mailto:Francois.Dahmani@univ-grenoble-alpes.fr)

---

### Lieu(x) ville

> Grenoble

---

### Campus

> Grenoble - Domaine universitaire