

# Cryptographie pour la cybersécurité

Formation dispensée par l'agence LEBESGUE de mathématiques pour l'innovation ([agence.lebesgue.fr](http://agence.lebesgue.fr)).

## CONTACTS

### Service Formation Continue et Alternance (SFCA)

6, rue Kléber CS 16926  
35069 Rennes CEDEX  
[formation-continue.univ-rennes1.fr](mailto:formation-continue.univ-rennes1.fr)

### Chargée de mission

**Florence MORFOISSE**  
[florence.morfoisse@univ-rennes1.fr](mailto:florence.morfoisse@univ-rennes1.fr)

### Assistante de formation

**Anne-Laure FUSELIER**  
[anne.fuselier-lemoine@univ-rennes1.fr](mailto:anne.fuselier-lemoine@univ-rennes1.fr)

### Responsable pédagogique

**Sylvain DUQUESNE**  
IRMAR, Centre Henri Lebesgue  
Université de Rennes 1

Responsable du Master  
"Mathématiques de l'information,  
cryptographie", Directeur de

l'Institut de Recherche  
MATHématiques de Rennes

## Publics

Cette formation courte s'adresse aux chercheurs, ingénieurs dans les entreprises et les laboratoires de recherche scientifique, en particulier en lien avec le domaine de la cybersécurité.

## Compétences développées

- S'approprier les enjeux de la cryptographie moderne et de son utilisation.
- Avoir une meilleure compréhension des méthodes de cryptographie utilisées en cybersécurité de nos jours pour pouvoir les comparer et choisir la plus adaptée au contexte.

## Organisation pédagogique

**Durée :** Ce cours se compose de 6 modules de 3 heures, chacun constitué d'un cours magistral (environ 2 heures) et d'une courte séance de mise en pratique sous Python et/ou Sage (environ 1 heure).

**Lieu de la formation :** campus de Beaulieu - Rennes

**Calendrier :** la formation se déroule les 28, 29 et 30 mars 2022.



AGENCE LEBESGUE  
DE MATHÉMATIQUES POUR L'INNOVATION





## PROGRAMME

- Histoire de la cryptographie et introduction à la cryptographie moderne.
- Infrastructures à clé publique.
- Systèmes de chiffrement par bloc : modes de chiffrement, chiffrements de Feistel, TP Vigenère+ présentation de l'AES.
- Le système RSA : principe, mise en oeuvre et attaques principales.
- Cryptographie basée sur le logarithme discret : présentation générale et comparaison avec RSA. Mise en oeuvre via les corps finis et les courbes elliptiques.
- Fonctions de hachage : utilisation, modèles de Merkle-Damgard et des fonctions éponges, présentation de SHA-3.
- Protocoles de signatures numériques.

## CANDIDATER

### Prérequis

- Niveau bac+2 en mathématiques, en particulier en algèbre (notion de groupe et de corps par exemple).
- Maîtrise de l'algorithmique et de la programmation de base en Python ou Sage.

### Prix de la formation

1 800 euros

### Pré-inscription en ligne

→ [formation-continue.univ-rennes1.fr/crypto](http://formation-continue.univ-rennes1.fr/crypto)