

# Cryptographie et sécurité - Syllabus#1

Mickael Bettinelli

Septembre 2022

## 1 Introduction

Le cours de cryptographie est divisé en trois séquences. Chaque séquence contient un CM, un TD et un TP de deux heures chacun. La première séquence se concentre sur les chiffrements symétriques et l'arithmétique modulaire. La deuxième sur les chiffrements asymétriques et de l'arithmétique modulaire plus poussé. La dernière séquence présente aux étudiants une ouverture sur des techniques et infrastructures plus larges et plus modernes utilisées en cryptographie de nos jours. Contrairement aux deux premières séquences, celle-ci ne contient pas de TD.

Séquence 1	Séquence 2	Séquence 3
CM - cryptographie symétrique et arithmétique modulaire	CM - cryptographie asymétrique et arithmétique modulaire	CM - infrastructures pour la cryptographie et codes correcteurs
TD -manipuler les chiffrements symétriques et arithmétique modulaire	TD -manipuler les chiffrements asymétriques et arithmétique modulaire	
TP - développer des techniques de crypto symétrique	TP - développer des techniques de crypto asymétrique	TP - mettre en place une infrastructure

Figure 1: Séquences du cours de cryptographie

Ce document a pour objectif de définir les compétences que les étudiants doivent avoir acquis à l'issue de la première séquence.

## 2 Quand

Encore à fixer, mais devrait se trouver semaines 45 et 46.

## 3 Comment

Les CM sont préparés de manière à favoriser l’interactivité avec les étudiants (outils types wooclap utilisés). Il est préférable que les étudiants aient accès soit un ordinateur personnel soit leur téléphone durant la séance.

Les TD papiers sont des salles de cours classiques où l’utilisation des ordinateurs et téléphones n’est pas souhaitable. En vue d’un enseignement explicite (à détailler dans les prochains jours), les étudiants doivent se regrouper par 3 pour travailler les exercices. Les enseignants doivent en permanence passer dans les groupes pour vérifier la bonne compréhension des étudiants en leur demandant d’explicitier leur raisonnement.

Les TD ordinateurs nécessitent des salles équipées de matériel informatique. Les étudiants peuvent travailler avec leur matériel personnel si souhaité. L’objectif de ces séances est le travail en autonomie.

## 4 Compétences requises avant la séquence

- Effectuer des calculs simples avec l’opérateur modulo
- Programmer en Python (conditions / boucles)

## 5 Compétences acquises après la séquence

- Faire des opérations sur un ensemble  $\mathbb{Z}/n\mathbb{Z}$
- Expliquer le fonctionnement du chiffrement symétrique
- Expliquer le fonctionnement des chiffrements par bloc et par flot
- Utiliser les bonnes méthodes de chiffrement en fonction du contexte applicatif
- Programmer un outil de chiffrement utilisant des méthodes abordées en cours en Python (César, Vigenère)

## 6 Evaluation

Toutes les séquences sont évaluées en semaine 49 de la même manière:

- une évaluation sur ordinateur de 2 heures en fin de module permet de vérifier l’acquisition des compétences par les étudiants.

- une évaluation papier (le contrôle final) également en fin de module pour valider les compétences théoriques.