Introduction à l'arithmétique

Code IA3, 6 ECTS, Semestre S3

Prérequis : Néant **Évaluation :** Contrôle continu et examen final

Mentions concernées : Mathématiques

Horaires hebdomadaires : 2 h CM + 3 h TD

Objectifs

Maîtrise de structures essentielles de l'arithmétique et de ses applications fondamentales notamment en cryptographie. Les notions abordées, fondamentales en mathématiques, apparaissent dans divers concours de recrutement.

Programme

1. Groupes cycliques et leurs sous-groupes.
2. Arithmétique dans $\mathbb{Z}$; division euclidienne, pgcd et ppcm, formule de Bézout, factorisation en nombres premiers.
3. Anneau $\mathbb{Z}/n\mathbb{Z}$, groupe des inversibles, indicateur d'Euler, lemme chinois, corps $\mathbb{Z}/p\mathbb{Z}$.
4. Algorithme RSA.