Sécurisation des données et cryptologie	Semestre 8	**Responsable :** Yassin EL HILLALI / Moad Dehbi

Objectifs de l'ECUE en termes de compétences et d'acquis d'apprentissage visés

À l'issue de cette UE, l'apprenant aura progressé sur les compétences suivantes du référentiel de la formation :

- BC1.1 : Comprendre et appliquer les concepts fondamentaux de la cryptographie et de la cryptanalyse.
- BC2.1 : Analyser les vulnérabilités des systèmes de chiffrement et proposer des solutions sécurisées.
- BC3.1 : Maîtriser les outils mathématiques nécessaires à la conception et à l'analyse de systèmes cryptographiques.
- BC4.1 : Concevoir et implémenter des systèmes cryptographiques symétriques et asymétriques

Plus précisément, il sera capable de :

- Expliquer la différence entre cryptographie symétrique et asymétrique.
- Appliquer des algorithmes de cryptographie, tels que le chiffre de César, Vigenère, RSA, et El Gamal.
- Utiliser des outils mathématiques, tels que la divisibilité, le théorème de Bézout et le théorème chinois, pour renforcer les systèmes de chiffrement.
- Analyser la sécurité des systèmes de chiffrement à clé publique et à clé secrète.

Description de l'ECUE

Cryptographie et Sécurité de l'Information

Introduction à la cryptographie

- Terminologie : cryptographie, cryptanalyse, cryptosystème
- Systèmes cryptographiques : symétriques et asymétriques
- Algorithmes de cryptographie (César, Vigenère, RSA, El Gamal)

Outils mathématiques pour la cryptographie

- Divisibilité et congruence
- Théorème de Bézout, Gauss, Fermat
- Inverse multiplicatif et PGCD

Cryptographie symétrique

- Chiffre de César et de Vigenère
- Analyse de la sécurité des systèmes à clé secrète

Cryptographie asymétrique

- RSA : génération des clés, chiffrement et déchiffrement
- Système El Gamal : génération de clés, algorithmes de chiffrement/déchiffrement

Algorithmes de sécurité avancés

- Théorème chinois
- Chiffrement Diffie-Hellman
- Chiffrement affine

Activités pédagogiques proposées

- Études de cas sur des attaques cryptographiques historiques et modernes.
- Analyse de la sécurité des systèmes cryptographiques existants (RSA, El Gamal, etc.).
- Implémentation d'algorithmes de chiffrement/déchiffrement en Python.
- Démonstration de la vulnérabilité des systèmes par cryptanalyse.
- Travaux pratiques : réalisation de tests de sécurité sur des systèmes cryptographiques.

Prérequis
Cours de mathématiques discrètes

Références