Cryptographie Avancée	Semestre 8	**Responsable :** Youcef IMINE

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

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

- BC2.2 : Étudier, comparer et sélectionner les outils et méthodes nécessaires à la conception, au développement et au test d'une solution informatique
- BC2.4 : Documenter une étude et une solution informatique
- BC2.5 : Analyser et identifier les aspects réglementaires et techniques
- BC3.1. Analyser une solution informatique et en mesurer les performances en utilisant les outils et métriques adaptés (réseaux, systèmes, accès aux données, sécurité, etc.)
- BC3.2 : Assurer et optimiser les performances des systèmes d'information
- BC3.3 : Proposer, planifier et développer des évolutions
- BC3.5. Fiabiliser et sécuriser
- BC4.3- Déployer une solution informatique

Plus précisément, il sera capable de :

- Choisir une bibliothèque cryptographique appropriée pour un projet de développement
- Créer une documentation technique pour une bibliothèque cryptographique
- Étudier les réglementations en vigueur en matière de cryptographie, en identifiant les exigences légales ou les normes à respecter
- Analyser les performances d'un algorithme de chiffrement symétrique en utilisant des outils de profilage et en mesurant des métriques telles que la vitesse de chiffrement et de déchiffrement, la consommation de mémoire et la consommation d'énergie
- Concevoir et implémenter une stratégie de gestion des clés cryptographiques pour assurer la sécurité et la disponibilité des clés utilisées dans un système informatique
- Développer une extension à une bibliothèque de cryptographie existante pour ajouter de nouvelles fonctionnalités ou prendre en charge de nouveaux algorithmes

- Sensibiliser les utilisateurs aux bonnes pratiques de sécurité en matière de cryptographie, telles que la gestion des mots de passe et la protection des clés privées
- Déployer des bibliothèques et des frameworks cryptographiques sur une plateforme

Description de l'ECUE

- Attaques et contre-mesures dans le chiffrement symétrique
- Attaques et contre-mesures dans le chiffrement asymétrique
- Méthodes cryptographiques avancées (chiffrement homomorphe, chiffrement fonctionnel, chiffrement basé sur les attributs, chiffrement basé sur l'identité, cryptographie à boîte blanche)

Prérequis

Concepts de sécurité, Cryptographie, Services et protocoles réseaux

Références

S. Ghernaouti : Cybersécurité (5e édition, Sécurité informatique et réseaux), Dunod, 2016.