

Cryptographie	Semestre 6	Responsable : François GOICHOT
----------------------	-------------------	---------------------------------------

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 : Etudier, comparer et sélectionner les outils et méthodes nécessaires à la conception, au développement et au test d'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.)
- BC3.5 : Fiabiliser et sécuriser

Plus précisément, il sera capable de :

- Distinguer les différentes méthodes et outils cryptographiques
- Comprendre les aspects techniques de la cryptographie
- Comprendre les principes et le fonctionnement des algorithmes de chiffrement
- Apprécier les apports et les limites des outils cryptographiques en terme de garantie de la sécurité
- Implémenter des algorithmes de chiffrement symétrique tels que AES et DES
- Identifier des modèles d'attaques classiques qui peuvent être contrées par des outils cryptographiques

Description de l'ECUE

- Présentation générale de la cryptographie (fonctions de base, apports et limites)
- Notion de complexité
- Fonctions de hachage

- Chiffrements symétrique (DES, AES) et asymétrique (RSA)

Prérequis

Mathématiques appliquées, développement d'applications.

Références

Gildas Avoine, Pascal Junod, Philippe Oechslin et Sylvain Pasini, Sécurité informatique, Vuibert, 3ème édition, 2015.