Nom de l'UE : Concepts de la sécurité	Semestre : S6

Objectifs de l'UE
Au terme de cette UE qui présente la terminologie et les concepts fondamentaux de la cybersécurité, l'étudiant saura : ● Distinguer et utiliser correctement les termes inhérents aux méthodes et outils organisationnels, réglementaires et techniques concourant à la garantie de la confidentialité, l'intégrité et la disponibilité du patrimoine informationnel constituant le système d'information (SI) d'un organisme. ● Appréhender la cybersécurité dans sa globalité en prenant en compte aussi bien les aspects technologiques que réglementaires et organisationnels ● Distinguer les différentes méthodes et outils cryptographiques. ● Comprendre les aspects techniques de la cryptographie ● Comprendre les principes et le fonctionnement des algorithmes de cryptage ● Apprécier les apports et les limites des outils cryptographiques en terme de garantie de la sécurité ● Identifier des modèles d'attaques classiques qui peuvent être contrées par des outils cryptographiques. ● Se baser sur les concepts de la cryptographie aussi bien asymétrique que symétrique pour déployer des solutions d'authentification forte.

Description des ECUE
Fondements de la sécurité • Notions de risque, vulnérabilité et attaque • Concepts fondamentaux de la cybersécurité (Confidentialité, Intégrité, Authentification) • Infrastructures à clé publique (PKI) • Concepts du triple A (AAA) et de non-répudiation • Distinction entre sécurité des données et sécurité périmétrique (IDS) **Cryptographie** • Présentation générale de la cryptographie (fonctions de base, apports et limites) • Notion de complexité • Fonctions de hachage • Chiffrements symétrique (DES, AES) et asymétrique (RSA)

Projet sécurité

Implémentation d'outils PKI pour l'authentification des accès à un serveur Web.

- Définir et mettre en place une infrastructure à clés publiques

Garantir des communications authentifiées et chiffrées pour l'utilisation d'un service (ex : serveur web)

Pré-requis

Mathématiques appliquées, développement d'applications.

Bibliographie

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