

Sécurité



En bref

Langue(s) d'enseignement: Français

Ouvert aux étudiants en échange: Non

Présentation

Objectifs

- 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 asymétrique pour déployer des solutions d'authentification forte.
- Découvrir les formalités obligatoires du Règlement Général sur la Protection des Données
- Définir les aspects juridiques du RGPD
- Comprendre l'importance des obligations du RGPD
- Préparer le plan d'actions de mise en conformité

Pré-requis obligatoires

Programmation système

Liste des enseignements

	Nature	CM	TD	TP	Crédits
Cryptographie	UE				
Fondements de la sécurité	UE				
Normes et RGPD	UE				