



5.00 crédits	30.0 h + 30.0 h	Q2
--------------	-----------------	----

Enseignants	Legat Benoît ;Peters Thomas ;
Langue d'enseignement	Anglais > Facilités pour suivre le cours en français
Lieu du cours	Louvain-la-Neuve
Préalables	Ce cours suppose acquises les notions de base telles qu'enseignées dans les cours : <ul style="list-style-type: none"> • LEPL1108 - Mathématiques discrètes et probabilités • LEPL1101 - Algèbre linéaire • LEPL1109 - Statistiques et science des données • LEPL1402 - Informatique II
Thèmes abordés	Le cours abordera différents thèmes fondamentaux en apprentissage et en cryptographie, et les outils mathématiques associés. Apprentissage: notions d'aléatoire et pseudo-aléatoire, échantillonnage, algorithmes probabilistes (Monte Carlo, hash maps, ...), éléments de théorie de l'information, inférence bayésienne, fondements statistiques de l'apprentissage. Cryptographie: notions de sécurité, primitives de base (fonctions pseudo-aléatoires, fonctions de hachage cryptographiques, chiffrement par bloc, ...), éléments de cryptographie symétrique, éléments de cryptographie à clé publique.
Acquis d'apprentissage	<p>A la fin de cette unité d'enseignement, l'étudiant est capable de :</p> <p>Au terme de cette unité d'enseignement, l'étudiant sera capable de:</p> <ul style="list-style-type: none"> • Comprendre et expliquer le rôle du hasard et de l'échantillonnage dans les algorithmes probabilistes et les méthodes de Monte Carlo, ainsi que leurs garanties de convergence. • Modéliser et analyser des problèmes statistiques et d'apprentissage à l'aide des outils de la théorie de l'information et de l'inférence bayésienne, en identifiant les liens entre incertitude, régularisation et généralisation. • Comprendre et expliquer comment les principes statistiques (biais-variance, régularisation, généralisation) guident la conception, l'évaluation et la robustesse des modèles d'apprentissage automatique. • Définir et expliquer les propriétés de sécurité visées par les primitives cryptographiques de base (confidentialité, authenticité, mise en accord de clé), et identifier les limites de ces propriétés • Comprendre comment sont conçues et fonctionnent les plus importantes primitives cryptographiques utilisées aujourd'hui (chiffrement par bloc, fonction de hachage cryptographique, ...) • Comprendre et expliquer comment ces primitives peuvent être composées en vue d'obtenir des protocoles de communication sécurisée. <p>Dans le contexte du référentiel d'acquis d'apprentissage du programme de bachelier ingénieur civil, ce cours contribuera aux axes suivants: AA 1.1, 1.2, AA 2.3, 2.4, 2.6</p>
Faculté ou entité en charge:	DACS

Programmes / formations proposant cette unité d'enseignement (UE)				
Intitulé du programme	Sigle	Crédits	Prérequis	Acquis d'apprentissage
Filière en Electricité	FILELEC	5		
Filière en Mathématiques Appliquées	FILMAP	5		
Mineure Polytechnique	MINPOLY	5		