UCLouvain

ldacs1110

2026

Foundations of Machine Learning and Cryptography

5.00 credits	30.0 h + 30.0 h	Q2

Teacher(s)	Legat Benoît ;Peters Thomas ;
Language :	English > French-friendly
Place of the course	Louvain-la-Neuve
Prerequisites	This course assumes prior knowledge of the basic concepts taught in the following courses: LEPL1108 - Discrete Mathematics and Probability LEPL1101 - Linear Algebra LEPL1109 - Statistics and Data Science LEPL1402 - Computer Science II
Main themes	The course will cover various fundamental topics in machine learning and cryptography, and the associated mathematical tools. Learning: concepts of randomness and pseudo-randomness, sampling, probabilistic algorithms (Monte Carlo, hash maps, etc.), elements of information theory, Bayesian inference, statistical foundations of machine learning. Cryptography: security concepts, basic primitives (pseudo-random functions, cryptographic hash functions, block ciphers, etc.), elements of symmetric cryptography, elements of public-key cryptography.
Learning outcomes	**At the end of this learning unit, the student is able to :** At the end of this course unit, students will be able to: • Understand and explain the role of randomness and sampling in probabilistic algorithms and Monte Carlo methods, as well as their convergence guarantees. • Model and analyze statistical and machine learning problems using the tools of information theory and Bayesian inference, identifying the links between uncertainty, regularization, and generalization. • Understand and explain how statistical principles (bias-variance, regularization, generalization) guide the design, evaluation, and robustness of machine learning models. • Define and explain the security properties targeted by basic cryptographic primitives (confidentiality, authenticity, key matching), and identify the limitations of these properties. • Understand how the most important cryptographic primitives used today are designed and function (block cipher, cryptographic hash function, etc.). • Understand and explain how these primitives can be combined to create secure communication protocols. Within the framework of the learning outcomes framework for the Bachelor of Civil Engineering program, this course will contribute to the following learning areas: AA 1.1, 1.2, AA 2.3, 2.4, 2.6
Content	FoL (partim A) • Concentration inequalities • Monte Carlo Methods and sampling (Gibbs, Metropolis, MCMC) • Randomness and pseudo-randomness, hash maps, leftover hash lemma • Information theory, Shannon entropy, mutual information, KL divergence, Fano • Bayesian inference (prior and posterior distributions,...) and causality • Generalization theory, PAC-Learning, sample complexity, compression, VC dimension • Gaussian process regression • Applications in learning FoC (partim B) This part will focus on the foundational aspects of the following topics: • Information theoretic security and impossibility results • Pseudo-random functions, hash functions, random oracles

	• Design and analysis of pseudo-random permutations • Symmetric encryption and message authentication codes • Public key agreement • Public key encryption and signatures
Faculty or entity in charge	DACS

Programmes containing this learning unit (UE)				
Program title	Acronym	Credits	Prerequisite	Learning outcomes
Specialization track in Electricity	FILELEC	5		🔍
Specialization track in Applied Mathematics	FILMAP	5		🔍
Mineure Polytechnique	MINPOLY	5		🔍