






5 crédits	30.0 h + 30.0 h	Q1
-----------	-----------------	----

Enseignants	Pereira Olivier coordinateur ;Standaert François-Xavier ;
Langue d'enseignement	Anglais
Lieu du cours	Louvain-la-Neuve
Préalables	Une familiarité avec les notions de base de la cryptographie est bienvenue.
Thèmes abordés	<p>Les thèmes discutés dans le cours évoluent d'année en année. Ces thèmes pourront inclure :</p> <ul style="list-style-type: none"> • le calcul sur des données chiffrées • la conception de bases de données pouvant être interrogées sans que le serveur hébergeant les données ne sache quelle donnée est lue • les systèmes de communication anonyme • les monnaies cryptographiques • le mélange de cartes sur internet • l'organisation d'élections dont les organisateurs ne sont pas en mesure de tricher • le contrôle d'accès ne permettant pas de tracer les utilisateurs • la compréhension d'attaques contre la confidentialité des données, y compris les attaques de dé-anonymisation et de ré-identification, le profilage et les attaques par canaux secondaires • l'appréhension des questions soulevées par la surveillance de masse et des manières d'y réagir.
Acquis d'apprentissage	<p>Contribution du cours au référentiel du programme</p> <ul style="list-style-type: none"> • - AA1.2, AA1.3, • AA2.2, AA2.3, AA2.5, • AA3.1, • AA5.1, AA5.3, AA5.4, AA5.6, • AA6.1, AA6.2, AA6.3 <p>¹ Acquis d'apprentissage spécifiques au cours</p> <p>A l'issue de ce cours, les étudiants seront capables de :</p> <ul style="list-style-type: none"> • analyser les risques d'attaques contre l'authenticité et la confidentialité des données dans un système complexe ; • comprendre les outils cryptographiques et architecturaux permettant de limiter ces risques ; • évaluer des mesures d'utilité et de confidentialité appliquées à des bases de données et à des systèmes distribués. <p>-----</p> <p><i>La contribution de cette UE au développement et à la maîtrise des compétences et acquis du (des) programme(s) est accessible à la fin de cette fiche, dans la partie « Programmes/formations proposant cette unité d'enseignement (UE) ».</i></p>
Modes d'évaluation des acquis des étudiants	L'examen final sera basé sur des exercices, en relation avec les acquis d'apprentissage décrits ci-dessus.
Méthodes d'enseignement	Cours magistraux et séances d'exercices.
Contenu	Différents thèmes seront discutés d'année en année. Ceux-ci pourront inclure : les calculs multi-parties sécurisés, les mémoires aveugles, le vote vérifiable, les monnaies cryptographiques, les réseaux de communications anonymes, les identifiants anonyme, la confidentialité différentielle et les big data, la cryptographie post-Snowden.
Ressources en ligne	https://moodleucl.uclouvain.be/course/view.php?id=11446
Bibliographie	Des transparents et des références sont disponibles sur le site Moodle du cours.

Faculté ou entité en charge:	ELEC
------------------------------	------

Programmes / formations proposant cette unité d'enseignement (UE)				
Intitulé du programme	Sigle	Crédits	Prérequis	Acquis d'apprentissage
Master [120] : ingénieur civil en science des données	DATE2M	5		
Master [120] : ingénieur civil en informatique	INFO2M	5		
Master [120] : ingénieur civil électricien	ELEC2M	5		
Master [120] en sciences informatiques	SINF2M	5		
Master [120] : ingénieur civil en mathématiques appliquées	MAP2M	5		
Master [120] en science des données, orientation technologies de l'information	DATI2M	5		