

<b>Intitulé de l'UE</b>	<b>Cryptologie</b>
<b>Section(s)</b>	- (3 ECTS) Master en Sciences de l'Ingénieur industriel / orientation Informatique / Cycle 2 Bloc 1

<b>Responsable(s)</b>	<b>Heures</b>	<b>Période</b>
Jean-Sébastien LERAT	24	Quad 1

<b>Activités d'apprentissage</b>	<b>Heures</b>	<b>Enseignant(s)</b>
Cryptographie et introduction à la Cryptanalyse	24h	Jean-Sébastien LERAT

<b>Prérequis</b>	<b>Corequis</b>

<b>Répartition des heures</b>
<b>Cryptographie et introduction à la Cryptanalyse</b> : 14h de théorie, 10h d'exercices/laboratoires

<b>Langue d'enseignement</b>
<b>Cryptographie et introduction à la Cryptanalyse</b> : Français, Anglais

<b>Connaissances et compétences préalables</b>
<ul style="list-style-type: none"> <li>• Notions de programmations</li> <li>• Mathématiques de l'enseignement secondaire</li> <li>• Mathématiques du/des bloc(s) précédent(s)</li> </ul>

<b>Objectifs par rapport au référentiel de compétences ARES</b>
<b>Cette UE contribue au développement des compétences suivantes</b>
<p><b>- Master en Sciences de l'ingénieur industriel :</b></p> <ul style="list-style-type: none"> <li>• Identifier, conceptualiser et résoudre des problèmes complexes <ul style="list-style-type: none"> <li>◦ Intégrer les savoirs scientifiques et technologiques afin de faire face à la diversité et à la complexité des problèmes rencontrés</li> <li>◦ Sélectionner et exploiter les logiciels et outils conceptuels les plus appropriés pour résoudre une tâche spécifique</li> <li>◦ Établir ou concevoir un protocole de tests, de contrôles et de mesures.</li> </ul> </li> <li>• Concevoir et gérer des projets de recherche appliquée <ul style="list-style-type: none"> <li>◦ Mener des études expérimentales, en évaluer les résultats et en tirer des conclusions</li> </ul> </li> <li>• S'engager dans une démarche de développement professionnel <ul style="list-style-type: none"> <li>◦ Réaliser une veille technologique dans sa sphère d'expertise</li> </ul> </li> </ul>
<p><b>- Master en Sciences de l'ingénieur industriel en Informatique :</b></p> <ul style="list-style-type: none"> <li>• Analyser, concevoir, implémenter et maintenir des systèmes informatiques logiciels et matériels <ul style="list-style-type: none"> <li>◦ Maîtriser et mettre en oeuvre les techniques de sécurité logicielle et matérielle (cryptologie, architectures d'authentifications, ...)</li> </ul> </li> </ul>

## Objectifs de développement durable (rubrique optionnelle pour l'année académique 2022-2023)



### **Education de qualité**

Objectif 4 Assurer l'accès de tous à une éducation de qualité, sur un pied d'égalité, et promouvoir les possibilités d'apprentissage tout au long de la vie

sous-objectifs : **4.3 - 4.4 - 4.7**



### **Egalité entre les sexes**

Objectif 5 Parvenir à l'égalité des sexes et autonomiser toutes les femmes et les filles

sous-objectifs : **5.b**



### **Energie propre et d'un coût abordable**

Objectif 7 Garantir l'accès de tous à des services énergétiques fiables, durables et modernes, à un coût abordable

sous-objectifs : **7.1 - 7.2 - 7.3**



### **Travail décent et croissance économique**

Objectif 8 Promouvoir une croissance économique soutenue, partagée et durable, le plein emploi productif et un travail décent pour tous

sous-objectifs : **8.2 - 8.3 - 8.4 - 8.5 - 8.6 - 8.8 - 8.b**



### **industrie, innovation et infrastructure**

Objectif 9 Bâtir une infrastructure résiliente, promouvoir une industrialisation durable qui profite à tous et encourager l'innovation

sous-objectifs : **9.1 - 9.2 - 9.3 - 9.4 - 9.5 - 9.b - 9.c**



### **Inégalités réduites**

Objectif 10 Réduire les inégalités dans les pays et d'un pays à l'autre

sous-objectifs : **10.2 - 10.4 - 10.7**



### **Villes et communautés durables**

Objectif 11 Faire en sorte que les villes et les établissements humains soient ouverts à tous, sûrs, résilients et durables

sous-objectifs : **11.4 - 11.6 - 11.a - 11.b**



### **Consommation et production responsables**

Objectif 12 Établir des modes de consommation et de production durables

sous-objectifs : **12.2 - 12.5 - 12.8**



### **Mesures relatives à la lutte contre les changements climatiques**

Objectif 13 Prendre d'urgence des mesures pour lutter contre les changements climatiques et leurs répercussions

sous-objectifs : **13.3**



### **Paix, justice et institutions efficaces**

Objectif 16 Promouvoir l'avènement de sociétés pacifiques et ouvertes aux fins du développement durable, assurer l'accès de tous à la justice et mettre en place, à tous les niveaux, des institutions efficaces, responsables et ouvertes

sous-objectifs : **16.6 - 16.b**



### **Partenariats pour la réalisation des objectifs**

Objectif 17 Renforcer les moyens de mettre en oeuvre le Partenariat mondial pour le développement durable et le revitaliser

sous-objectifs : **17.7 - 17.14 - 17.17**

#### **Acquis d'apprentissage spécifiques**

- Citer et décrire les algorithmes cryptographiques/stéganographiques modernes
- Décrire l'évolution de la cryptographie
- Expliquer le fonctionnement de la signature électronique, du Darknet, des monnaies virtuelles
- Résoudre des exercices cryptographiques/stéganographiques simples sans dispositif électronique
- Comparer et critiquer les différents algorithmes vus au cours
- Justifier le choix d'un procédé de communication sûr

#### **Contenu de l'AA Cryptographie et introduction à la Cryptanalyse**

- Terminologie et historique de la cryptographie
- Les algorithmes classiques de la cryptographie (AES, RSA, ...)
- Les différentes méthodes de la cryptographie et les problèmes des clés.
- La cryptanalyse
- La signature électronique
- La stéganographie
- Le Darknet
- Les monnaies virtuelles
- Cryptographie des communications sans fil
- Cryptographie quantique
- Cryptographie homomorphe

#### **Méthodes d'enseignement**

**Cryptographie et introduction à la Cryptanalyse** : cours magistral, approche par situation problème, approche avec TIC, utilisation de logiciels

#### **Supports**

**Cryptographie et introduction à la Cryptanalyse** : copies des présentations, syllabus

#### **Évaluations et pondérations**

<b>Évaluation</b>	Note globale à l'UE
<b>Langue(s) d'évaluation</b>	Français
<b>Méthode d'évaluation</b>	20% évaluation continue non remédiable 80% examen écrit

#### **Report de note d'une année à l'autre pour l'AA réussie en cas d'échec à l'UE**

Cryptographie et introduction à la Cryptanalyse : **non**

