

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

Responsable(s)	Heures	Période
Jean-Sébastien LERAT	25	Quad 1

Activités d'apprentissage	Heures	Enseignant(s)
Cryptographie et introduction à la Cryptanalyse	25h	Jean-Sébastien LERAT

Prérequis	Corequis

Répartition des heures
<b>Cryptographie et introduction à la Cryptanalyse</b> : 15h de théorie, 10h d'exercices/laboratoires

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

Connaissances et compétences préalables
<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>

Objectifs par rapport au référentiel de compétences ARES
<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>

### 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
- 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

### 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**

Année académique : **2019 - 2020**