HEH be Sciences et technologies

8a avenue Maistriau
7000 Mons

www.heh.be

| Intitulé de l'UE | Cryptologie |
|---|---|
| Section(s) | - **(3 ECTS)** 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 |
|---|
| **Cryptographie et introduction à la Cryptanalyse :** 15h de théorie, 10h d'exercices/laboratoires |

| Langue d'enseignement |
|---|
| **Cryptographie et introduction à la Cryptanalyse :** Français, Anglais |

## Connaissances et compétences préalables

- Notions de programmations
- Mathématiques de l'enseignement secondaire
- Mathématiques du/des bloc(s) précédent(s)

## Objectifs par rapport au référentiel de compétences ARES

**Cette UE contribue au développement des compétences suivantes**

**- Master en Sciences de l'ingénieur industriel :**

- Identifier, conceptualiser et résoudre des problèmes complexes
  - Intégrer les savoirs scientifiques et technologiques afin de faire face à la diversité et à la complexité des problèmes rencontrés
  - Sélectionner et exploiter les logiciels et outils conceptuels les plus appropriés pour résoudre une tâche spécifique
  - Établir ou concevoir un protocole de tests, de contrôles et de mesures.
- Concevoir et gérer des projets de recherche appliquée
  - Mener des études expérimentales, en évaluer les résultats et en tirer des conclusions
- S'engager dans une démarche de développement professionnel
  - Réaliser une veille technologique dans sa sphère d'expertise

**- Master en Sciences de l'ingénieur industriel en Informatique :**

- Analyser, concevoir, implémenter et maintenir des systèmes informatiques logiciels et matériels
  - Maîtriser et mettre en oeuvre les techniques de sécurité logicielle et matérielle (cryptologie, architectures d'authentifications, …)

**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**

| | |
|---|---|
| **Évaluation** | Note globale à l'UE |
| **Langue(s) d'évaluation** | Français |
| **Méthode d'évaluation** | 20% évaluation continue non remédiable<br><br>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 : **2020 - 2021**