







|           |                 |    |
|-----------|-----------------|----|
| 5 crédits | 30.0 h + 15.0 h | Q1 |
|-----------|-----------------|----|

|   |  |
|---|--|
| Enseignants                                 | Pereira Olivier ;  |
| Langue d'enseignement                       | Anglais  |
| Lieu du cours                               | Louvain-la-Neuve   |
| Préalables                                  | Notions élémentaires d'algèbre (telles que proposées dans les cours LMAT1131 ou LFSAB1101 par exemple) et de probabilités (telles que proposées dans les cours LMAT1271 ou LFSAB1105 par exemple).   |
| Thèmes abordés                              | On introduira les concepts fondamentaux de la cryptographie moderne, en accordant une attention particulière aux aspects mathématiques et algorithmiques. Des problèmes et constructions historiques seront abordés, qui serviront de base à la présentation des notions de sécurité et algorithmes les plus utilisés aujourd'hui, ainsi qu'à la justification de leur sécurité.   |
| Acquis d'apprentissage                      | <p>Contribution du cours aux acquis d'apprentissage du programme de master en mathématique.</p> <p>A la fin de cette activité, l'étudiant aura progressé dans sa capacité à :</p> <ul style="list-style-type: none"> <li>- Connaître et comprendre un socle fondamental des mathématiques. Il aura notamment développé sa capacité à :                     <ul style="list-style-type: none"> <li>-- Reconnaître les concepts fondamentaux d'importantes théories mathématiques actuelles.</li> <li>- Faire preuve d'abstraction, de raisonnement et d'esprit critique. Il aura notamment développé sa capacité à :                             <ul style="list-style-type: none"> <li>-- Dégager les aspects unificateurs de situations et expériences différentes.</li> <li>-- Reasonner dans le cadre de la méthode axiomatique.</li> <li>-- Construire et rédiger une démonstration de façon autonome, claire et rigoureuse.</li> </ul> </li> </ul> </li> </ul> <p>Acquis d'apprentissage spécifiques au cours.</p> <p>A la fin de cette activité, l'étudiant sera capable de :</p> <ol style="list-style-type: none"> <li>1 - Décrire, de manière rigoureuse, la fonction et les propriétés de sécurité des principales primitives utilisées en cryptographie.</li> <li>- Construire des attaques ou des preuves de la sécurité d'algorithmes.</li> <li>- Reconnaître et articuler les principales techniques de cryptographie mises en oeuvre pour sécuriser l'information.</li> <li>- Déterminer l'existence d'algorithmes offrant certaines garanties de sécurité dans différents contextes, notamment sur base de résultats d'impossibilité.</li> </ol> <p>Modes d'évaluation des acquis des étudiants</p> <p>L'évaluation se fait sur base d'un examen écrit. La possibilité est offerte aux étudiants, durant l'examen, de présenter oralement leurs solutions aux questions proposées.</p> <p>On teste la connaissance et la compréhension des notions, des exemples et des principaux algorithmes introduits durant le cours, ainsi que la capacité à évaluer la sécurité d'algorithmes cryptographiques, que ce soit de manière constructive (rédaction de preuves de sécurité) ou destructive (description d'attaques). L'étudiant peut choisir la langue de l'examen (anglais ou français).</p> <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'évaluation se fait sur base d'un examen écrit.<br>L'étudiant peut répondre aux questions en anglais ou en français.  |
| Méthodes d'enseignement                     | Le cours est donné sous forme de cours magistral et de séances de travaux pratiques.<br>Une attention particulière est consacrée à l'analyse des liens entre les concepts théoriques introduits dans le cours et les applications pratiques de la cryptographie.   |
| Contenu                                     | On introduira les concepts fondamentaux de la cryptographie moderne, en accordant une attention particulière aux aspects mathématiques et algorithmiques. Des problèmes et constructions historiques seront abordés, qui   |

|                              |  |
|------------------------------|--|
|                              | <p>serviront de base à la présentation des notions de sécurité et algorithmes les plus utilisés aujourd'hui, ainsi qu'à la justification de leur sécurité.</p> <ul style="list-style-type: none"> <li>- Éléments de théorie de l'information, chiffrement parfait.</li> <li>- Algorithmes probabilistes, sécurité calculatoire, modèles d'attaquants, élaboration et usage de preuves de sécurité en cryptographie.</li> <li>- Chiffrement symétrique: notions de sécurité, constructions élémentaires, DES, AES, cryptanalyse, modes opératoires.</li> <li>- Codes d'authentification, fonctions de hachage.</li> <li>- Cryptographie asymétrique: protocole de Diffie-Hellman, chiffrement (RSA, ElGamal, ...), signature (RSA, hash-and-sign, DSS, ...), infrastructure à clé publique.</li> <li>- Éléments de théorie algorithmique des nombres (arithmétique modulaire, test de primalité, courbes elliptiques).</li> <li>- Protocoles : challenge-response, identification, authentification, protocoles à divulgation nulle.</li> <li>- Standards et normes : élaboration et précautions à prendre en pratique.</li> </ul> <p>L'équilibre entre les différentes parties est susceptible de varier d'année en année.</p> |
| Ressources en ligne          | Site <a href="#">Moodle</a> .  |
| Bibliographie                | <ul style="list-style-type: none"> <li>• Slides</li> </ul> <p>J. Katz et Y. Lindell, Introduction to Modern Cryptography, (Chapman and Hall/CRC Press).<br/>More references are available on Moodle.</p>   |
| Faculté ou entité en charge: | MATH   |

| Programmes / formations proposant cette unité d'enseignement (UE) |           |         |           |   |
|---|-----------|---------|-----------|---|
| Intitulé du programme   | Sigle     | Crédits | Prérequis | Acquis d'apprentissage  |
| Master [120] en sciences mathématiques                            | MATH2M    | 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       |           |  |
| Approfondissement en sciences mathématiques                       | LMATH100P | 5       |           |  |