Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB6003 Gr. 01
Titre : Techniques de cryptographie
Session : Hiver 2026 Horaire et local
Professeur : de Lima Sobreira, Péricles

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e sera initiée aux concepts de la cryptographie et de son application dans le domaine de la sécurité des données. Elle/Il pourra analyser différents algorithmes cryptographiques en évaluant leur sécurité, efficacité et complexité, ainsi que d'acquérir une compréhension générale des méthodes de cryptanalyse.

Contenu

Introduction à la cryptographie. Exemples historiques des techniques de cryptologies classiques : le chiffrement de Vigenère, le chiffrement de Hill; la cryptanalyse des crypto-systèmes classiques. La cryptographie moderne. Cryptographie à clé secrète; D.E.S., triple DES, AES, etc.; modes d'opération des chiffrements par blocs. Cryptographie à clé publique : RSA, El-Gamal, etc. Protocoles cryptographiques : authentification, distribution de clés. Fonctions de hachage : algorithmes SHA-1 et MD5.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

L'objectif de ce cours est de doter les étudiant.es des compétences nécessaires pour comprendre, analyser et appliquer divers algorithmes de cryptographie et de cryptanalyse, en évaluant leur robustesse et efficacité dans le contexte de la sécurité des données.

3. Stratégies pédagogiques :

Les formules pédagogiques suivantes seront utilisées :

- Les connaissances seront présentées sous forme de cours magistraux;
- Le matériel pédagogique sera mis à la disposition des étudiant(e)s sur Moodle;
- Un forum de discussion sera aussi mis à la disposition des étudiant(e)s, afin de leur permettre de poser leurs questions et, le cas échéant, de contribuer à l'élaboration de réponses.

Les cours seront réalisés en mode présentiel. Les travaux à terme devront être remis aux dates indiquées. Aucun retard ne sera toléré.

4. Heures de disponibilité ou modalités pour rendez-vous :

Consultation au bureau sur rendez-vous, via courriel, ou via Zoom (envoyer un courriel à pericles.delimasobreira@uqo.ca)

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Introduction à la cryptographie • Aperçu de la cryptographie • Contexte historique et exemples de cryptographie classique • Importance de la cryptographie dans la sécurité des données	14 janvier 2026

2	Techniques de cryptographie classique • Le chiffrement par substitution et transposition • Le chiffrement de Vigenère • Le chiffrement de Hill	21 janvier 2026
3	Cryptanalyse des systèmes classiques • Introduction à la cryptanalyse • Recherche exhaustive de clé • Cryptanalyse linéaire	28 janvier 2026
4	Cryptanalyse des systèmes classiques (suite) • Analyse de fréquence • Étude de cas : briser le chiffre de Vigenère	04 février 2026
5	Cryptographie à clé secrète et DES • Fondamentaux des chiffrements par bloc • Modes d'opération des chiffrements par blocs • DES et Triple DES • Cryptanalyse linéaire (suite)	11 février 2026
6	Standard de Chiffrement Avancé (AES) • Introduction à l'AES • Bourrage et modes d'opération à l'AES • Mécanismes de chiffrement/déchiffrement à l'AES Révision pour l'examen mi-session	18 février 2026
7	**Examen de mi-session**	25 février 2026
8	**Semaine d'études**	04 mars 2026
9	Cryptographie à clé publique • Concepts de base pour la cryptographie à clé publique • L'algorithme RSA et ses fondements • Sécurité et génération de clés RSA • Cryptosystème El-Gamal	11 mars 2026
10	Fonctions de hachage et leurs propriétés • Algorithmes MD5 et SHA-1 • Résistance aux collisions et sécurité des fonctions de hachage • Paradoxe des anniversaires	18 mars 2026
11	Fonctions de hachage et leurs propriétés (suite) • Introduction à SHA-2 • Principes de conception des fonctions de hachage	25 mars 2026
12	Protocoles cryptographiques • Authentification et distribution de clés • Protocoles d'échange de clés Diffie-Hellman	1er avril 2026
13	Sécurité des protocoles et TLS • Sécurité des protocoles de communication • Introduction à SSL et TLS	8 avril 2026
14	Révision pour l'examen final Bilan de la matière	15 avril 2026
15	**Examen final**	22 avril 2026

6. Évaluation du cours :

L'évaluation est l'appréciation du niveau d'apprentissage atteint par l'étudiant(e) par rapport aux objectifs des cours et des programmes.

Dans le cas spécifique du cours **Techniques de cryptographie**, l'attribution des notes se fera selon la répartition suivante :

- Examen de mi-session (individuel) : 30 % (25 février 2026)
- Examen final (individuel) : 40 % (22 avril 2026)
- Listes d'exercices (individuel ou en groupe) : 30 %

Les examens seront réalisés en présentiel (pavillon Lucien-Brault).

Carte d'étudiant OBLIGATOIRE aux journées des examens.

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

Tolérance ZÉRO en matière de violence à caractère sexuel.

Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.

Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.

Ensemble, participons à une culture de respect.

Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

8. Principales références :

- Notes du cours (diapos, tutoriels, exercices, etc.), disponibles sur Moodle.
- Lafourcade, P.; More, M. 25 énigmes ludiques pour s'initier à la cryptographie. 2e éd. Dunod, 2024.
- Vergnaud, D. Exercices et problèmes de cryptographie. 4e éd. Dunod, 2023.
- Lafourcade, P.; Onete, C. 20 énigmes ludiques pour se perfectionner en cryptographie. Dunod, 2023.
- Katz, J.; Lindell, Y. Introduction to modern cryptography. 3rd ed. CRC Press, 2020.
- Stinson, D. R.; Paterson, M. B. Cryptography: Theory and Practice. 4th ed. CRC Press, 2019.
- Barthélemy, P.; Rolland, R.; Véron, P. Cryptographie : principes et mises en œuvre. 2e éd. Hermes Science, 2012.

9. Page Web du cours :

https://moodle.uqo.ca