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

Sigle : CYB6003 Gr. 02
Titre : Techniques de cryptographie
Session : Automne 2026 Horaire et local
Professeur : Frédéric Lesage

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;

Le cours est offert principalement en présentiel (les modalités de cours et d'évaluation sont sujettes à modification selon l'évolution de la situation sanitaire). Toutefois, les séances des 12, 19 et 26 novembre 2026 seront offertes en mode non-présentiel synchrone sur Zoom, selon l'horaire habituel. Le lien de connexion sera communiqué sur Moodle. Toutes les autres séances, y compris les examens, se dérouleront en présentiel.

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

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

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Cours 1 - Fondements mathématiques de la cryptographie** • Cryptosystèmes, représentation des données et arithmétique modulaire • Chiffrements affine et de César • Recherche exhaustive, analyse fréquentielle et complexité	11 septembre 2026

2	**Cours 2 - Cryptographie classique et cryptanalyse** • Chiffrements de Vigenère et de Hill • Chiffrements homophonique, par transposition et hybride • Cryptanalyse des systèmes classiques	17 septembre 2026
3	**Cours 3 - Sécurité parfaite et outils de calcul cryptographique** • Masque jetable et sécurité parfaite de Shannon • Réutilisation des clés et sécurité calculatoire • Exponentiation binaire modulaire et complexité	24 septembre 2026
4	**Cours 4 - DES, Triple DES et réseaux de Feistel** • Chiffrements par blocs, confusion, diffusion et effet d'avalanche • Réseaux de Feistel, structure de DES et boîtes de substitution • Triple DES et principales attaques	1 oct. 2026
5	**Cours 5 - AES et modes d'opération** • Arithmétique dans le corps fini GF(2^8) • Transformations et génération des sous-clés d'AES • Modes ECB, CBC, CTR et chiffrement authentifié AES-GCM	8 oct. 2026
6	*Semaine d'études*	15 octobre 2026
7	*Examen mi-session*	22 octobre 2026
8	**Cours 6 - Diffie-Hellman, ElGamal et distribution de clés** • Groupes cycliques et problème du logarithme discret • Échange de clés Diffie-Hellman et attaque de l'homme du milieu • Cryptosystème ElGamal et distribution hybride des clés	29 octobre 2026
9	**Cours 7 - RSA, signatures et authentification** • Fondements arithmétiques et preuve de correction de RSA • Sécurité, remplissage et attaques contre RSA sans protection • Signatures numériques, certificats et authentification	5 nov. 2026
10	**Cours 8 - Fonctions de hachage et authentification** • Préimages, secondes préimages, collisions et paradoxe des anniversaires • MD5, SHA-1, SHA-2 et introduction à SHA-3 • HMAC, dérivation de clés et application aux chaînes de blocs	12 nov. 2026 Non-présentiel
11	**Cours 9 - Fondements mathématiques de la cryptographie quantique** • Qubits, mesure, opérateurs unitaires et produits tensoriels • États de Bell et codage superdense • Non-clonage, distribution quantique de clés et effets de Shor et Grover	19 nov. 2026 Non-présentiel
12	**Cours 10 - Mathématiques de l'apprentissage quantum-ready** • Espaces complexes, produits hermitiens et calcul de Wirtinger • Optimisation de pertes réelles sur des paramètres complexes • Noyaux hermitiens et noyaux quantiques	26 nov. 2026 Non-présentiel
13	*Examen final*	3 déc. 2026

14	**Présenations orales**	10 décembre 2026
15	**Présenation orales**	17 décembre 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 %
- Examen final (individuel) : 40 %
- Présentation orale : 30 %

Les examens seront réalisés en présentiel (pavillon Lucien-Brault), à livre fermé (vous n'avez besoin que de quoi écrire et effacer ; je fournis le papier). 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, etc.), disponibles sur Moodle.
- Stinson, D. R.; Paterson, M. Cryptography: Theory and Practice, 4th edition, CRC Press, 2019
- Lafourcade, P.; More, M. 25 énigmes ludiques pour s'initier à la cryptographie. Dunon, 2021
- Lafourcade, P.; Onete, C. 20 énigmes ludiques pour se perfectionner en cryptographie. Dunod, 2023
- Lindell, Y.; Katz, J. Introduction to modern cryptography, 2nd edition. CRC Press, 2018
- Véron, P.; Rolland, R.; Barthélemy, P. Cryptographie : principes et mises en œuvre. 2ème édition (revue et augmentée). Hermes Science, 2012

9. Page Web du cours :

https://moodle.uqo.ca