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

Sigle : INF6293 Gr. 01
Titre : Éléments avancés en cryptographie
Session : Automne 2025 Horaire et local
Professeur.e : Bouhaddi, Myria

1. Description du cours paraissant à l'annuaire :

Objectifs

Maîtriser les techniques avancées de cryptologie répondant à des critères spécifiques de sécurité et de performance. Apprendre et maîtriser les fondements mathématiques et l'analyse de ces techniques et leurs implications sur la sécurité.

Contenu

Rappel sur les systèmes de chiffrement symétriques et asymétriques. Rappel des notions d'algèbre et de théorie des nombres. Cryptographie basée sur les logarithmes discrets (cryptographie à courbes elliptiques, ElGamal, DSA, échange de clés Diffie-Hellman, etc.). Fonctions de hachage (MD5, SHA-1, etc.). Cryptographie à seuil. Cryptographie basée sur l'identité. Cryptanalyse. Partage de secrets. Éléments de cryptographie quantique.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

- Maîtriser les techniques avancées de cryptologie répondant à des critères spécifiques de sécurité et de performance.
- Analyser les algorithmes cryptographiques modernes, leurs forces, leurs vulnérabilités et leurs domaines d'application.
- Évaluer les implications pratiques et sécuritaires des techniques étudiées, y compris dans un contexte post-quantique.

3. Stratégies pédagogiques :

Les séances de cours seront présentées sous forme magistrales, parsemées d'exercices de compréhension. Le matériel pédagogique est accessible à partir de la plateforme Moodle dédiée au cours. Un forum de discussion sera aussi disponible pour poser des questions liées à la matière enseignée.

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

Communication par courriel (myria.bouhaddi@uqo.ca) et via le forum de discussion. Rencontres sur Zoom.

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Introduction et perspectives contemporaines en cryptographie** • Historique et rôle de la cryptographie aujourd'hui. • Typologie : symétrique vs asymétrique, probabiliste vs déterministe. • Modèles de sécurité : IND-CPA, IND-CCA • Introduction à la cryptographie classique • Chiffrements par substitution et transposition : mono et poly alphabétique, Vigenère, Hill.	03 sep 2025
2	**Cryptanalyse de la cryptographie classique** • Introduction à la cryptanalyse • Limites des algorithmes classiques face aux attaques modernes. • Cas d'étude : cassure du chiffre de Vigenère. • Transition vers la nécessité de la cryptographie moderne.	10 sep 2025

3	**Cryptographie symétrique (Partie 1) : DES et variantes** • DES : structure de Feistel, substitutions et permutations, fonctionnement détaillé. • Vulnérabilités : taille de clé réduite, attaques par force brute. • 2DES et 3DES : motivation, fonctionnement, renforcement de la sécurité. • Attaque Meet-in-the-Middle sur 2DES.	17 sep 2025
4	**Cryptographie symétrique (Partie 2) : AES, modes et authentification** • AES : structure (SubBytes, ShiftRows, MixColumns, AddRoundKey), différences avec Feistel. • Modes de chiffrement : ECB, CBC, CFB, OFB, CTR, GCM ; chiffrement authentifié et AEAD. • HMAC : principe et usage. • Vulnérabilités courantes : padding oracle, IV non aléatoire. Cas d'usage : TLS, stockage chiffré.	24 sep 2025
5	**Cryptographie asymétrique (partie 1): fondements, RSA et Diffie-Hellman** • Rappels mathématiques : arithmétique modulaire, petit théorème de Fermat, théorème d'Euler, groupes cycliques, générateurs, logarithme discret. • RSA : génération de clés, chiffrement/déchiffrement, sécurité, attaques classiques. • Diffie-Hellman : protocole, sécurité, attaque de l'homme du milieu.	01 oct 2025
6	**Cryptographie asymétrique (Partie 2) : ElGamal et DSA** • ElGamal : principe, chiffrement probabiliste, preuve IND-CPA. • DSA : signature, vérification, risques liés au nonce. • Comparaison RSA / ElGamal / DH : usages et contraintes. • Applications et limites : o Usage dans OpenPGP, anciens protocoles SSL. o Taille de clé pour sécurité équivalente à RSA.	08 oct 2025
7	**Semaine d'études**	15 oct 2025
8	**Examen de mi-session**	22 oct 2025
9	**Cryptographie sur les courbes elliptiques (ECC)** • Avantages de l'ECC : courtes clés, performance • Cryptosystèmes : o ECDH (échange de clé) o ElGamal-ECC (chiffrement) o ECDSA (signature) • Sélection de courbes : NIST, Curve25519, Brainpool • Applications : blockchain, mobiles, Signal	29 oct 2025

10	**Fonctions de hachage et HMAC** • Propriétés : préimage, seconde préimage, collision • Algorithmes : MD5 (cassé), SHA-1 (affaibli), SHA-2, SHA-3 • Attaques sur MD5/SHA1 • HMAC : principe et sécurité • Cas d'usage : stockage de mots de passe, Git, blockchain	05 nov 2025
11	**Cryptographie à seuil et partage de secrets** • Schéma de Shamir • Reconstruction du secret • Schémas à seuil (t-out-of-n) • Applications : cryptographie distribuée, wallets, systèmes de backup **(Séance en non-présentiel)**	12 nov 2025
12	**Cryptographie avancée : homomorphique, fonctionnelle et MPC** • Chiffrement homomorphe partiel et complet (Paillier, BGV, TFHE) • Chiffrement fonctionnel : attributs, politiques (ABE) • Calcul multipartite sécurisé (MPC) • Cas d'usage : vote électronique, apprentissage sur données chiffrées **(Séance en non-présentiel)**	19 nov 2025
13	**Algorithmes modernes et cryptographie post-quantique** • Limites des algorithmes classiques (RSA, ECC) face aux attaques quantiques, avec focus sur l'algorithme de Shor et sa complexité. • Étude de cas : factorisation via Shor et comparaison avec les meilleures méthodes classiques. • Panorama des algorithmes post-quantiques (Kyber, Dilithium, McEliece) et analyse de leur résistance face aux ordinateurs quantiques.	26 nov 2025
14	**Présentation des projets**	03 dec 2025
15	**Examen final**	10 dec 2025

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 Éléments avancés en cryptographie, l'attribution des notes se fera selon la répartition suivante :

- Examen de mi-session : 30 %
- Examen final : 40 %
- Travail de session : 30 % (les dates pour les remises des livrables du projet de session seront discutées avec les étudiants en salle de cours)

7. Politiques départementales et institutionnelles :

- Politiques relatives à la tenue des examens
- Note sur le plagiat et les fraudes
- 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 :

- Katz, J., & Lindell, Y. (2020). *Introduction to modern cryptography* (3rd ed.). CRC Press.
- Stinson, D., Vaudenay, S., Avoine, G., & Junod, P. (2003). *Cryptographie : Théorie et pratique* (2e éd.). Vuibert.
- Paar, C., & Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Springer.
- Goldreich, O. (2004). *Foundations of cryptography, Volume 2*. Cambridge University Press.

9. Page Web du cours :

https://moodle.uqo.ca