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

Sigle : CYB6003 Gr. 01
Titre : Techniques de cryptographie
Session : Hiver 2025 Horaire et local
Professeur : Bouhaddi, Myria

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 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 à la cryptographie • Aperçu de la cryptographie • Contexte historique et exemples de cryptographie classique • Importance de la cryptographie dans la sécurité des données	14 jan 2025
2	Techniques de cryptographie classique • Le chiffrement par substitution et transposition • Le chiffrement de Vigenère • La machine Enigma • Le chiffrement de Hill	21 jan 2025

3	Cryptanalyse des systèmes classiques • Introduction à la cryptanalyse • Recherche exhaustive de clé • Cryptanalyse linéaire	28 jan 2025
4	Cryptanalyse des systèmes classiques (suite) • Analyse de fréquence • Étude de cas : briser le chiffre de Vigenère	04 fév 2025
5	Cryptographie à clé secrète et DES • Fondamentaux des chiffrements par bloc • DES et Triple DES • Modes d'opération des chiffrements par blocs	11 fév 2025
6	Standard de chiffrement avancé (AES) • Introduction à AES et ses mécanismes • Modes d'opération d'AES	18 fév 2025
7	Cryptographie à clé publique • L'algorithme RSA et ses fondements • Sécurité et génération de clés RSA • Cryptosystème El-Gamal Révision pour l'examen mi-session	25 fév 2025
8	Semaine d'études	04 mar 2025
9	**Examen de mi-session**	11 mar 2025
10	Fonctions de Hachage et leurs propriétés • Algorithmes SHA-1 et MD5 • Résistance aux collisions et sécurité des fonctions de hachage	18 mar 2025
11	Fonctions de Hachage et leurs propriétés (suite) • Introduction à SHA-2 • Principes de conception des fonctions de hachage **(Séance en non-présentiel)**	25 mar 2025
12	Protocoles cryptographiques • Authentification et distribution de clés • Protocoles d'échange de clés Diffie-Hellman et RSA **(Séance en non-présentiel)**	01 avr 2025
13	Sécurité des protocoles et TLS • Introduction à TLS et SSL • Sécurité des protocoles de communication Révision pour l'examen final	08 avr 2025
14	Présentation des projets	15 avr 2025
15	**Examen final**	22 avr 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 **Techniques de 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 :

- 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 :

- Stinson, D., Vaudenay, S., Avoine, G., & Junod, P. (2003). *Cryptographie-Théorie et pratique/2ème édition*. vuibert.
- Lindell, Y.; Katz, J. Introduction to modern cryptography, 2nd edition. CRC Press, 2018
- Goldreich, O. (2004). *Foundations of Cryptography, Volume 2*. Cambridge: Cambridge University press.

9. Page Web du cours :

https://moodle.uqo.ca