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

Sigle : CYB6003 Gr. 01
Titre : Techniques de cryptographie
Session : Automne 2024 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 modalités de cours et d'évaluation sont sujettes à modification selon l'évolution de la situation sanitaire). 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	4 septembre 2024

2	Techniques de Cryptographie Classique • Le chiffrement par substitution et transposition • Le chiffrement de Vigenère • Le chiffrement de Hill	11 septembre 2024
3	Cryptanalyse des systèmes classiques • Introduction à la cryptanalyse • Recherche exhaustive de clé • Cryptanalyse linéaire	18 septembre 2024
4	Cryptanalyse des systèmes classiques (suite) • Analyse de fréquence • Étude de cas : briser le chiffre de Vigenère	25 septembre 2024
5	Cryptographie à Clé Secrète et DES • Fondamentaux des chiffrements par bloc • DES et Triple DES • Modes d'opération des chiffrements par blocs	2 octobre 2024
6	Standard de Chiffrement Avancé (AES) • Introduction à AES et ses mécanismes • Modes d'opération d'AES Révision pour l'examen mi-session	9 octobre 2024
7	Semaine d'études	16 octobre 2024
8	**Examen de mi-session**	23 octobre 2024
9	Cryptographie à Clé Publique • L'algorithme RSA et ses fondements • Sécurité et génération de clés RSA • Cryptosystème El-Gamal	30 octobre 2024
10	Fonctions de Hachage et leurs propriétés • Algorithmes SHA-1 et MD5 • Résistance aux collisions et sécurité des fonctions de hachage	6 novembre 2024
11	Fonctions de Hachage et leurs propriétés (suite) • Introduction à SHA-2 • Principes de conception des fonctions de hachage	13 novembre 2024
12	Protocoles Cryptographiques • Authentification et distribution de clés • Protocoles d'échange de clés Diffie-Hellman et RSA	20 novembre 2024
13	Sécurité des Protocoles et TLS • Introduction à TLS et SSL • Sécurité des protocoles de communication Révision pour l'examen final	27 novembre 2024
14	Présentation des projets	4 décembre 2024

15	**Examen final**	11 décembre 2024

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 % (23 octobre 2024)
- Examen final : 40 % (11 décembre 2024)
- Travail de session : 30 % (les dates pour les remises des livrables du projet de session seront discutées avec les étudiants en salle de cours)

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. Une moyenne inférieure à 50 % aux examens est éliminatoire et conduit automatiquement à un échec.

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