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

Sigle : CYB1163 Gr. 01
Titre : Cryptographie
Session : Été 2025 Horaire et local
Professeur : Frédéric LESAGE

1. Description du cours paraissant à l'annuaire :

Objectifs
Au terme de ce cours, l'étudiant.e sera initié.e aux concepts fondamentaux liés au domaine de la cryptologie et sera familier.e avec différents domaines d'application de la cryptographie.

Contenu
Histoire de la cryptographie et de la cryptanalyse. Protocoles cryptographiques (authentification, distribution de clés, etc.). Systèmes cryptographiques symétriques (DES, AES, RC4, etc.). Systèmes cryptographiques asymétriques (RSA, DSA, Elgamal, Courbes elliptiques, etc.). Infrastructure à clé publique. Cryptographie homomorphe. Sécurité des algorithmes cryptographiques (complexité algorithmique, implémentation, etc.). Cryptographie post-quantique. Fonctions de hachage (MD5, SHA-1, etc.). Cryptanalyse. Applications (SSL/TLS, PGP, commerce électronique, chaîne de blocs "blockchain", etc.). Ce cours comporte des séances obligatoires de travaux pratiques (TP).

2. Stratégies pédagogiques :

La formule pédagogique utilisée dans ce cours comprend les éléments suivants :
Cours magistraux (une période de 3 heures par semaine).

1. Dix Quiz.
2. Trois Examens.

Cours en présentiel avec disponibilité par zoom.

- **Pour les rencontres en mode non-présentiel sur ZOOM. Les détails de la réunion Zoom sont disponibles sur la page Moodle du cours**
- Examens
- Disponibilité d'une page MOODLE contenant le matériel du cours et les résultats des évaluations.

Liens et guides utiles :

- Guide d'utilisation de Zoom à l'intention des étudiants

3. Site pour soutien de réussite en mode non-présentiel : uqo.ca/etudier-non-presentiel.

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

Disponible sur rendez-vous par :
- Zoom,
- Courriel : frederic.lesage@uqo.ca,
- Teams
- et au bureau B-2030 Lucien Brault

5. Plan détaillé du cours sur 7,5 semaines :

Séance	Thèmes	Dates
1	• Présentation du plan de cours • Introduction à la Cryptographie • Chiffre Affine, Code César et Clef symétrique	06 mai 2025

2	• Crypto-système symétrique DES
	• Python : notions de base pour la cryptographie
	  ○ Mapping et les uplets
	• Algèbre de Boole
	  ○ Quiz 1
	  ▪ TP 1 12 mai 2025
		08 mai 2025

3	• Arithmétique modulaire • Code masque-jetable ○ Quiz 2	13 mai 2025

4	• Théorie des nombres – les premiers
	• Clef Deffie-Hellman
	  ○ Quiz 3
	  ▪ TP 2 16 mai 2025
		15 mai 2025

5	**Examen 1**	20 mai 2025

6	• Clefs publiques
	• Crypto-système RSA
	• Preuve de l'exactitude RSA
	  ○ Quiz 4
	  ▪ TP 3 23 mai 2025
	  ▪ TP 4 26 mai 2025
		22 mai 2025

7	• Crypto-systèmes asymétriques • Sécurité RSA • Cryptographie homomorphe ○ Quiz 5	27 mai 2025

8	• Zoom
	• Crypto-systèmes à courbes elliptiques
	• TLS (Transport Layer Security)
	• Sécurité des algorithmes cryptographiques en ligne
	  ○ Quiz 6
	  ▪ TP 5 30 mai 2025
	  ▪ TP 6 02 juin 2025
		29 mai 2025

9	**Examen 2**	03 juin 2025

10	• Zoom
	• Crypto-analyse
	• hachage cryptographique
	• Blockchain et Cryptomonnaies
	  ○ Quiz 7
	  ▪ TP 7 06 juin 2025
	  ▪ TP 8 09 juin 2025
		05 juin 2025

11	• Cryptographie quantique • Données complexes et la notion du Qubit • Les opérateurs quantiques et le Hadamard ○ Quiz 8	10 juin 2025
12	• Circuit Quantique et l'état Bell • Codage avec Qiskit • Superdense coding	12 juin 2025

	○ Quiz 9	
13	• Quantum key distribution (QKD) • Protocol BB84 ○ Quiz 10	17 juin 2025
14	**Examen 3**	19 juin 2025

6. Évaluation du cours :

Outils d'évaluation	Pondération
Quiz	40 %
Examen 1	20 %
Examen 2	20 %
Examen 3	20 %

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.

8. Principales références :

- Christof Paar, Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners, Springer Berlin Heidelberg, 2011.
- Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. An Introduction to Mathematical Cryptography, Springer New York, 2008.
- Nigel P Smart. Cryptography An Introduction, McGraw-Hill, 2003.
- Neal Koblitz. A Course in Number Theory and Cryptography, Springer New York, 2012

9. Page Web du cours :

https://moodle.uqo.ca