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

Sigle : CYB1163 Gr. 01
Titre : Cryptographie
Session : Été 2026 **Horaire et local**
Professeur : David Caissy

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).

Descriptif - Annuaire

2. Objectifs spécifiques du cours :

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.

3. Stratégies pédagogiques :

Les stratégies pédagogiques suivantes seront utilisées, en **mode présentiel** :

- Cours magistraux
- Discussions de groupe
- Études de cas et travaux pratiques
- Examen de mi-session
- Examen final

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

Communications par courriel à l'adresse : **david.caissy@uqo.ca**. Périodes de consultation flexibles sur rendez-vous.

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Histoire de la cryptographie** • Cryptographie, cryptologie et cryptanalyse • Systèmes cryptographiques antiques • Cryptographie classique	5 mai 2026

2	**Introduction à la cryptographie moderne**
	• Objectifs fondamentaux de la sécurité de l'information
	• Fondements mathématiques de la cryptographie
	  ◦ Opérations binaires
	  ◦ Arithmétique modulaire
	  ◦ Logarithme discret
	
	Travail pratique 1 : Fondements mathématiques de la cryptographie (11 mai 2026)
		7 mai 2026

3	**Fonctions de hachage cryptographiques** • Propriétés des fonctions de hachage • Principaux algorithmes de hachage • Algorithme de hachage à clé • Attaques par collision	12 mai 2026
4	**Réseaux de permutation-substitution** • Chiffrement par blocs • Substitutions • Permutations • Génération de sous-clés	14 mai 2026
5	**Chiffrement symétrique** • Modèle de chiffrement symétrique • DES, 3DES et AES • Modes d'opération	19 mai 2026

6	**Chiffrement asymétrique**
	• Propriétés du chiffrement asymétrique
	• Algorithmes :
	  ◦ RSA
	  ◦ Diffie-Hellman
	  ◦ DSA
	
	Travail pratique 2 : Substitutions et permutations (25 mai 2026)
		21 mai 2026

7	**Examen de mi-session**	26 mai 2026
8	**Cryptographie à courbes elliptiques** • Introduction aux courbes elliptiques • ECDSA • Elliptic-curve Diffie–Hellman (ECDH) **Travail pratique 3 :** Chiffrement de données (1er juin 2026)	28 mai 2026
9	**Infrastructure à clé publique** • Infrastructure PKI • Autorités de certification • Certificats X.509	2 juin 2026
10	**Cryptographie appliquée** • Sécurité des communications • Chiffrement des données au repos • Système de gestion des clés • Cryptomonnaies **Travail pratique 4 :** Certificats de sécurité (8 juin 2026)	4 juin 2026

11	**Protocoles d'authentification**
	• Signatures numériques
	• Protocoles d'authentification :
	  ◦ SAML
	  ◦ OAuth 2.0
	  ◦ OIDC
		9 juin 2026

12	**Protection des mots de passe** • Solutions de sécurité adaptées aux mots de passe • Utilisation de sels • Attaques contre les mots de passe **Travail pratique 5 :** Attaque contre les mots de passe (15 juin 2026)	11 juin 2026

13	**Cryptanalyse**
	• Cryptographie homomorphe
	• Cryptanalyse statistique
	• Attaques par :
	  • Force brute
	  • Texte clair connu
	  • Texte chiffré
	  • Texte clair choisi
		16 juin 2026

14	**Cryptographie post-quantique** • Introduction à l'informatique quantique • Vulnérabilités des systèmes actuels • Familles d'algorithmes post-quantiques	18 juin 2026
15	**Examen final**	23 juin 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 **Cryptographie**, l'attribution des notes se fera selon la répartition suivante :

- **Examen de mi-session : 30 %**
- **Examen final : 40 %**
- **5 travaux pratiques : 30 % (6% chacun)**

7. Politiques départementales et institutionnelles :

(Cliquer sur le texte souligné pour ouvrir le lien)

- Politique relative à l'administration des examens écrits dans les cours de premier cycle
- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Règlement concernant le plagiat et la fraude
- Politique linguistique
- Procédure en cas d'absence aux évaluations : Cadre de gestion | Formulaire d'absence

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 :

- Christof Paar, Jan Pelzl, Tim Güneysu. ***Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms Second Edition***, Springer Berlin Heidelberg, 2024.
- Jean-Philippe Aumasson. ***Serious Cryptography, 2nd Edition: A Practical Introduction to Modern Encryption***, No Starch Press, 2025.

9. Page Web du cours :

https://moodle.uqo.ca