Université de Sherbrooke

Département d'informatique

IFT 606 – Sécurité et cryptographie

Plan d'activité pédagogique

Hiver 2026

Enseignant	Mohamed Mehdi Najjar
Courriel :	mohamed.mehdi.najjar@usherbrooke.ca
Local :	D4-1010-12
Téléphone :	+1 819 821-8000 x62260
Disponibilités :	À déterminer au début de la session. Au besoin, prendre rendez-vous par courriel.

Site web du cours : https ://moodle.usherbrooke.ca

Horaire

Exposé magistral :	Mercredi	10 h 30 à 11 h 20	salle D7-2023
	Jeudi	14 h 30 à 16 h 20	salle D7-2023

Description officielle de l'activité pédagogique[1]

Cibles de formation :	Être capable d'évaluer et de gérer les risques et la sécurité d'un système informatique. Être capable de définir une politique de sécurité. Savoir comment assurer la confidentialité et l'intégrité des données. Connaître les divers types d'attaques et leurs parades.
Contenu :	Concepts de base de la sécurité informatique. Confidentialité. Authentification. Intégrité. Contrôle des accès. Cryptographie. Signature électronique. Certificats. Gestion de clés. Attaques et parades. Virus. Architectures. Coupe-feu. Réseaux virtuels privés. Politiques de sécurité. Méthodologies, normes et analyse de risques.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Préalable	MAT115
Concomitant	IFT585
Particularités	Aucune

[1] https ://www.usherbrooke.ca/admission/fiches-cours/ift606

1 Présentation

Cette section présente les cibles de formation spécifiques et le contenu détaillé de l'activité pédagogique. Cette section, non modifiable sans l'approbation du comité de programme du Département d'informatique, constitue la version officielle.

1.1 Mise en contexte

L'informatisation est une tendance dans tous les domaines. Les non-informaticiens ne réalisent pas à quel point les risques de sécurité sont différents. L'accès et les échanges des données confidentielles sont rapides, faciles et invisibles en comparaison aux anciennes méthodes : le contexte a changé.

La sécurité informatique se définit comme suit : c'est l'état dans lequel l'information est hors de danger. En tant qu'analyste informatique, vous aurez à assurer la sécurité de l'information contenue dans les systèmes dont vous aurez la responsabilité.

Le cours de sécurité et cryptographie vous permettra de comprendre les menaces informatiques, les moyens pour les contrer, pour les prévenir et pour réagir le cas échéant. De plus, vous verrez de manière plus globale, comment favoriser et définir des environnements plus sécuritaires.

1.2 Cibles de formation spécifiques

À la fin du cours, un étudiant ou une étudiante doit être capable de :

1. connaître les principaux enjeux de la sécurité ;
2. comprendre les mécanismes de cryptographie et leur utilité ;
3. savoir mettre en pratique les connaissances selon le contexte ;
4. connaître les types d'attaques informatiques et leurs impacts ;
5. connaître les moyens de défense contre ces attaques ;
6. identifier les vulnérabilités des architectures et les solutions ;
7. connaître le processus d'enquête informatique ;
8. prendre conscience d'enjeux spécifiques de l'industrie ;
9. savoir communiquer.

1.3 Contenu détaillé

Thème	Contenu	Nbr. d'heures	Objectifs
1	Introduction : contexte et objectifs	2	1
2	Cryptographie : historique ; chiffrements : symétrique, asymétrique ; cryptographie appliquée	10	2, 3
3	Attaques : contexte ; vulnérabilités ; types d'attaques ; outils ; processus ; applications pratiques	10	3, 4
4	Défenses : défense vs types d'attaques ; défense vs architecture ; défense organisationnelle et facteur humain ; les meilleures pratiques	10	5, 6
5	Architecture de sécurité : défense et principes ; standards ; exemples pratiques	3	6, 8, 9
6	Enquête informatique	2	7

2 Organisation

Cette section propre à l'approche pédagogique de chaque enseignante ou enseignant présente la méthode pédagogique, le calendrier, le barème et la procédure d'évaluation ainsi que l'échéancier des travaux. Cette section doit être cohérente avec le contenu de la section précédente.

2.1 Méthode pédagogique

Une semaine typique consiste en trois (3) heures de cours magistral et six (6) heures de travail personnel. Chaque semaine, il y aura des exposés magistraux décrivant la théorie ainsi que des exemples développés en classe, au tableau. Des exercices réalisés aussi en classe, seront directement intégrés, au besoin, dans les cours magistraux. Deux séries d'exercices de révision, préparatoires pour les examens (périodique et final) seront fournies et corrigées, en classe.

2.2 Calendrier

Semaine	Commençant le	Thème
1	2026-01-05	1
2	2026-01-12	1 et 2
3	2026-01-19	2
4	2026-01-26	2
5	2026-02-02	2
6	2026-02-09	2 et 3
7	2026-02-16	3
8	2026-02-23	Semaine des examens périodiques
9	2026-03-02	Relâche
10	2026-03-09	3
11	2026-03-16	3 et 4
12	2026-03-23	4
13	2026-03-30	4 et 5
14	2026-04-06	5 et 6
15	2026-04-13	Examen
16	2026-04-20	Semaine des examens finals
17	2026-04-27	Semaine des examens finals

2.3 Évaluation

Type de l'évaluation	Pondération	Utilisation des IAG[1]
Devoirs (2)	30 %	Interdite 🔴
Examen intra	30 %	Interdite 🔴
Examen final	40 %	Interdite 🔴

[1] Référez-vous à la page "Balises d'utilisation des outils d'intelligence artificielle générative" à la fin du document.

Le cours comprend également des travaux pratiques (devoirs) à réaliser en laboratoire, avec le langage de programmation Python ou C++ (à spécifier au début de la session). Les devoirs devront être réalisés obligatoirement par équipe de deux (2) à quatre (4) personnes étudiantes . Le nombre exact sera précisé au début de la session selon l'effectif réel. Les devoirs seront à remettre sur la page Moodle du cours, au plus tard à la date butoir indiquée dans le devoir en question. Une (1) seule journée de retard sera tolérée avec une pénalité de 20 % (2 points).

Les critères d'évaluation pour les épreuves (travaux et examens) sont principalement basés sur la structure et clarté du code source (s'il y a lieu), l'exactitude et la précision des réponses aux questions théoriques ainsi que la pertinence des solutions proposées aux problèmes énoncés. La note de passage est le cumul des notes des évaluations, qui doit être supérieur ou égal à 50 sur 100. La cote finale sera attribuée dynamiquement par rapport à la performance globale du groupe.

2.3.1 Qualité de la langue et de la présentation

Conformément à l'article 17 du Règlement facultaire d'évaluations des apprentissages[2] l'enseignante ou l'enseignant peut retourner à l'étudiante ou à l'étudiant tout travail non conforme aux exigences quant à la qualité de la langue et aux normes de présentation.

2.3.2 Plagiat

Le plagiat consiste à utiliser des résultats obtenus par d'autres personnes afin de les faire passer pour sien et dans le dessein de tromper l'enseignante ou l'enseignant. Vous trouverez en annexe un document d'information relatif à l'intégrité intellectuelle qui fait état de l'article 9.4.1 du Règlement des études[3]. Lors de la correction de tout travail individuel ou de groupe une attention spéciale sera portée au plagiat. Si une preuve de plagiat est attestée, elle sera traitée en conformité, entre autres, avec l'article 9.4.1 du Règlement des études de l'Université de Sherbrooke. L'étudiante ou l'étudiant peut s'exposer à de graves sanctions qui peuvent être soit l'attribution de la note E ou de la note zéro (0) pour un travail, un examen ou une activité évaluée, soit de reprendre un travail, un examen ou une activité pédagogique. Tout travail suspecté de plagiat sera transmis au Secrétaire de la Faculté des sciences. Ceci n'indique pas que vous n'ayez pas le droit de coopérer entre deux équipes, tant que la rédaction finale des documents et la création du programme restent le fait de votre équipe. En cas de doute de plagiat, l'enseignante ou l'enseignant peut demander à l'équipe d'expliquer les notions ou le fonctionnement du code qu'elle ou qu'il considère comme étant plagié. En cas d'incertitude, ne pas hésiter à demander conseil et assistance à l'enseignante ou l'enseignant afin d'éviter toute situation délicate par la suite.

2.4 Échéancier des travaux

Devoirs	Sujet	Réception	Remise	Points
Devoir 1	Cryptographie	2026-01-26	2026-02-13	15
Devoir 2	Sécurité	2026-03-09	2026-04-03	15

[2] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/2017-10-27_Reglement_facultaire_-_evaluation_des_apprentissages.pdf

[3] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

2.5 Utilisation d'appareils électroniques et du courriel

Selon le règlement complémentaire des études, section 4.2.3 [4], l'utilisation d'ordinateurs, de cellulaires ou de tablettes pendant une prestation est interdite à condition que leur usage soit explicitement permise dans le plan de cours.

Dans ce cours, l'usage de téléphones cellulaires, de tablettes ou d'ordinateurs est autorisé. Cette permission peut être retirée en tout temps si leur usage entraîne des abus.

Tel qu'indiqué dans le règlement universitaire des études, section 4.2.3[5], toute utilisation d'appareils de captation de la voix ou de l'image exige la permission de la personne enseignante.

Note : Je réponds aux questions posées par courriel à l'extérieur des périodes de cours.

La messagerie du Moodle du cours est destinée aux interactions entre les personnes étudiantes. Communiquer avec l'enseignant exclusivement par courriel.

3 Matériel nécessaire pour l'activité pédagogique

Il n'y a pas de manuel obligatoire. Chacun des livres ci-dessous propose une approche spécifique de traiter une partie (thème) du contenu du cours.

4 Références

[1] Katz, Jonathan and Lindell, Yehuda : *Introduction to modern cryptography*. CRC press, 2020.

[2] Menezes, Alfred J and Van Oorschot, Paul C and Vanstone, Scott A : *Handbook of applied cryptography*. CRC press, 2018.

[3] Pfleeger, CP and Pfleeger, SL and Margulies, M : Security in Computing, Prentice Hall. *Boston–MA, USA*, 2006.

[4] Stallings, William and Brown, Lawrie and Bauer, Michael D and Bhattacharjee, Arup Kumar : *Computer security : principles and practice*. Pearson Education Upper Saddle River, NJ, USA, 2012.

[4] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/Sciences_Reglement_complementaire.pdf

[5] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

Faculté des sciences UdS

Délits relatifs aux études

Extrait du règlement des études (Règlement 2575-009)

Sont notamment considérés comme un délit relatif aux études les faits suivants :

a) commettre un plagiat, soit faire passer ou tenter de faire passer pour sien, dans une production évaluée, le travail d'une autre personne, des passages ou idées tirés de l'œuvre d'autrui ou du contenu, de toute forme, généré par un système d'intelligence artificielle (ce qui inclut notamment le fait de ne pas indiquer la source et la référence adéquate);
b) commettre un autoplagiat, soit soumettre, sans autorisation préalable, une même production, en tout ou en partie, à plus d'une activité pédagogique ou dans une même activité pédagogique (notamment en cas de reprise);
c) usurper l'identité d'une autre personne ou procéder à une substitution de personne lors d'une production évaluée ou de toute autre prestation obligatoire;
d) fournir ou obtenir toute forme d'aide non autorisée, qu'elle soit collective ou individuelle (incluant l'assistance provenant d'un système d'intelligence artificielle), pour une production faisant l'objet d'une évaluation;
e) obtenir par vol ou toute autre manœuvre frauduleuse, posséder ou utiliser du matériel non autorisé de toute forme (incluant le matériel numérique et celui généré par un système d'intelligence artificielle) avant ou pendant une production faisant l'objet d'une évaluation;
f) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique;
k) posséder ou avoir à sa portée un appareil électronique ou numérique interdit durant une activité d'évaluation;

[...]

Un guide sur l'intégrité intellectuelle vous est rendu disponible par le service des bibliothèques et des archives de l'Université de Sherbrooke, afin de bien comprendre les différents délits et ainsi éviter d'être aux prises avec un dossier disciplinaire et une ou des sanctions.

Les mesures pouvant être imposées à titre de sanctions disciplinaires sont les suivantes :

a) la réprimande simple ou sévère consignée au dossier étudiant pour la période fixée par l'autorité disciplinaire ou à défaut, définitivement. En cas de réprimande fixée pour une période déterminée, la décision rendue demeure au dossier de la personne aux seules fins d'attester de l'existence du délit en cas de récidive;
b) l'obligation de reprendre une production ou une activité pédagogique, dont la note pourra être établie en tenant compte du délit survenu antérieurement;
c) la diminution de la note ou l'attribution de la note E ou 0;

[...]

UDS Faculté des sciences

Balises d'utilisation des outils d'intelligence artificielle générative

Autorisés ou pas dans les situations d'apprentissage et d'évaluation ?

NIVEAU 0	NIVEAU 1	NIVEAU 2	NIVEAU 3	NIVEAU 4
L'utilisation des outils d'intelligence artificielle générative (IAg) est limitée, voire complètement interdite parce que la personne enseignante considère que l'usage de ces outils nuit au développement de compétences essentielles. Ces compétences peuvent être disciplinaires, comme elles peuvent être d'ordre méthodologique, rédactionnel ou informationnel. Considérant que l'utilisation des IAg requiert un esprit critique, il peut s'agir d'une situation d'apprentissage ou d'évaluation sans IAg qui vise à développer celui-ci. Dans ces situations, **la personne étudiante produit le travail**.			L'utilisation prononcée des IAg est permise parce que la personne enseignante considère que les personnes étudiantes sont en mesure d'exercer un esprit critique et sont capables de juger de la qualité des contenus produits par les IAg. Ou encore, l'utilisation est encouragée parce que la situation d'apprentissage ou d'évaluation proposée contribue à développer leur esprit critique. Dans ces situations, l'IAg produit le travail préliminaire, alors que **la personne étudiante s'assure de sa qualité en l'améliorant**.	
				
Utilisation interdite	**Utilisation limitée**	**Utilisation guidée**	**Utilisation balisée**	**Utilisation libre**
Le **NIVEAU 0** signifie que l'**utilisation est interdite**. Ceci signifie que si la personne enseignante a un motif de croire qu'il y a eu l'utilisation d'une IAg dans une situation d'évaluation, elle doit dénoncer les faits auprès de la personne responsable des dossiers disciplinaires universitaires. Il s'agit d'un délit relatif aux études tel que stipulé dans le Règlement des études.	Le **NIVEAU 1 D'UTILISATION** signifie que l'**utilisation est autorisée uniquement pour assister l'apprentissage dans le domaine disciplinaire ou des langues**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation peut être considérée comme un délit. Par exemple : Domaine disciplinaire : - S'inspirer - Générer des idées - Explorer un sujet pour mieux le comprendre - Générer du matériel pour apprendre Domaine des langues : - Identifier ses erreurs et se les faire expliquer - Reformuler un texte - Générer un plan pour aider à structurer un texte - Traduire un texte	Le **NIVEAU 2 D'UTILISATION** signifie que l'**utilisation est autorisée pour améliorer un travail produit par la personne étudiante**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Analyser des contenus - Obtenir une rétroaction - Évaluer la qualité de son travail à partir de critères - Demander à être confronté relativement à ses idées, à sa démarche - Diriger les processus de résolution de problèmes	Le **NIVEAU 3 D'UTILISATION** signifie que l'**utilisation est autorisée pour produire un travail qui sera amélioré.** Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Résumer ou rédiger des parties d'un texte - Générer un texte ou un modèle d'une production et l'adapter - Réaliser des calculs mathématiques - Produire du code informatique - Résoudre des problèmes complexes - Répondre à une question - Générer des images, ou autres contenus multimédias	Le **NIVEAU 4 D'UTILISATION** signifie qu'**aucune restriction spécifique n'est imposée**. Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Ce niveau inclut tout ce qui précède, de l'exploration à la production, ainsi que toute autre tâche particulière jugée complexe.

UDS Faculté des sciences

À considérer avant l'utilisation d'outils d'intelligence artificielles génératives

Si, en tant que personne étudiante envisagez d'utiliser un outil d'intelligence artificielle générative (IAG) lorsque l'évaluation autorise les niveaux 1 à 4 d'utilisation mentionnés précédemment.

Dans ce cas, gardez à l'esprit les éléments clés suivants.

- Vous assumez la responsabilité de tout le contenu produit, avec ou sans IAG, et intégré à votre production.
- Les produits des outils d'IAG peuvent très souvent comporter **des erreurs ou des faussetés** (hallucinations) : on doit donc impérativement valider tout contenu généré par ces outils.
- Dans l'état actuel de la Loi sur le droit d'auteur du Canada, les **productions faites par l'IAG sont du domaine public,** puisque les outils d'IAG ne sont pas reconnus comme des auteurs au sens de la Loi et que les contenus générés ne répondent pas aux critères d'une œuvre protégée, notamment aux critères d'originalité.
- L'entreprise qui fournit le service pourrait émettre certaines exigences dans ses conditions d'utilisation. Comme l'algorithme et le code informatique appartiennent à l'entreprise qui les a développés, nous devons tenir compte de ces conditions. Celles-ci pourraient également fournir des précisions relatives à la **réutilisation des données soumises (confidentialité)**.

Comment déclarer l'utilisation d'outils d'intelligence artificielle générative

Dans l'esprit d'une conduite intègre et responsable, vous devez TOUJOURS mentionner de façon explicite toute utilisation de l'intelligence artificielle, conformément au Règlement des études (9.4.1 Délits relatifs aux études). De plus, à des fins pédagogiques, il est recommandé de toujours intégrer à la production les requêtes, de même que les réponses intégrales générées par les outils d'IAG. Celles-ci pourront être intégrées directement dans le corps du texte ou en note de bas de page. Les réponses longues pourraient être insérées en annexe de votre document ou dans des documents supplémentaires, selon les directives de la personne enseignante.

L'utilisation de ces deux documents s'avèrera utile, ils se trouvent sous licence libre, donc vous pouvez utiliser les tableaux et les adapter selon votre besoin:

1. Modèle de citation : Ce formulaire, à remplir par l'enseignant, donne un exemple aux étudiants de citation de l'IAg dans la réalisation d'un travail évalué ou non.
2. Déclaration d'usage : Ce formulaire, à remplir par les étudiants, doit être remis avec une réalisation afin de déclarer l'usage de l'IAg dans la réalisation, qu'elle soit évaluée ou non.

Référence

La Faculté des sciences tient à remercier le SSF pour la production des documents.

- Cabana, M. et Côté, J.-A. (2024). Balises d'utilisation des outils d'intelligence artificielle générative. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. et Beaudet, M. (2024). Directives de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. (2024). Formulaire de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.