Université de Sherbrooke

Département d'informatique

IFT 606 – Sécurité et cryptographie

Plan d'activité pédagogique

Été 2024

Enseignant	Mohamed Mehdi Najjar
Courriel :	Mohamed.Mehdi.Najjar@USherbrooke.ca
Local :	
Téléphone :	+1 819 580-1274 x62876
Disponibilités :	À déterminer au début de la session. Au besoin, prendre rendez-vous par courriel.

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

Horaire

Groupe 1 :	Exposé magistral :	Lundi	8h30 à 9h20	salle D3-2029
		Mardi	8h30 à 10h20	salle D4-2024
Groupe 18 :	Exposé magistral :	Jeudi	11h00 à 11h50	salle L1-5615/L1-3670/L1-4665
		Jeudi	13h30 à 15h20	salle L1-5615/L1-3670/L1-4665

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	MAT 115
Concomitant	IFT 585
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	Travaux
1	Introduction : • Contexte • Objectifs et évaluation	2	1	
2	Cryptographie : • Historique • Chiffrement symétrique • Chiffrement asymétrique • Cryptographie appliquée	10	2, 3	✔
3	Attaque : • Contexte • Vulnérabilités • Types d'attaques • Outils • Le processus • Applications pratiques (laboratoire)	10	3, 4	✔
4	Défense : • Défense vs les types d'attaques • Défense vs l'architecture • Défense organisationnelle et facteur humain • 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 heures de cours magistral et six heures de travail personnel. Chaque semaine, il y aura des exposés magistraux décrivant la théorie ainsi que des exemples développés au tableau. Des exercices réalisés en classe, seront directement intégrés, au besoin, dans les cours magistraux. Des séries d'exercices de révision, préparatoires pour les examens (périodique et final) seront fournies et corrigées, en classe.

2.2 Calendrier

Semaine	Date	Thème
1	2024-04-29	1
2	2024-05-06	1 et 2
3	2024-05-13	2
4	2024-05-20	2
5	2024-05-27	2
6	2024-06-03	2 et 3
7	2024-06-10	3
8	2024-06-17	Examen périodique
9	2024-06-24	
10	2024-07-01	3
11	2024-07-08	3 et 4
12	2024-07-15	4
13	2024-07-22	4 et 5
14	2024-07-29	5 et 6
15	2024-08-05	Examen final
16	2024-08-12	Examen final

2.3 Évaluation

Devoirs (2)	30 %
Examen intra	30 %
Examen final	40 %

Le cours comprend également des travaux pratiques (devoirs) à réaliser en laboratoire, avec le langage de programmation Python. Les devoirs devront être réalisés obligatoirement par équipe de deux (2) à quatre (4) étudiantes et étudiants. 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 un cumul, des notes des évaluations, 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'évaluation 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

Les dates de remise des travaux seront indiquées sur les énoncés.

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 autorisées. 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.

3 Matériel nécessaire pour l'activité pédagogique

Il n'y a pas de manuel obligatoire. Chacun des livres ci-dessous propose une manière différente de traiter une partie 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.

[2] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/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/

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

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

UNIVERSITÉ DE SHERBROOKE

L'intégrité intellectuelle passe, notamment, par la reconnaissance des sources utilisées.
À l'Université de Sherbrooke, on y veille!

Extrait du *Règlement des études* (Règlement 2575-009)

9.4.1 DÉLITS RELATIFS AUX ÉTUDES

Un délit relatif aux études désigne tout acte trompeur ou toute tentative de commettre un tel acte, quant au rendement scolaire ou une exigence relative à une activité pédagogique, à un programme ou à un parcours libre.

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 ou des passages ou des idées tirés de l'œuvre d'autrui (ce qui inclut notamment le fait de ne pas indiquer la source d'une production, d'un passage ou d'une idée tirée de l'œuvre d'autrui);

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 aide non autorisée, qu'elle soit collective ou individuelle, pour une production faisant l'objet d'une évaluation;

e) obtenir par vol ou toute autre manœuvre frauduleuse, posséder ou utiliser du matériel de toute forme (incluant le numérique) non autorisé 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;

[…]

Par plagiat, on entend notamment :

- Copier intégralement une phrase ou un passage d'un livre, d'un article de journal ou de revue, d'une page Web ou de tout autre document en omettant d'en mentionner la source ou de le mettre entre guillemets;
- reproduire des présentations, des dessins, des photographies, des graphiques, des données… sans en préciser la provenance et, dans certains cas, sans en avoir obtenu la permission de reproduire;
- utiliser, en tout ou en partie, du matériel sonore, graphique ou visuel, des pages Internet, du code de programme informatique ou des éléments de logiciel, des données ou résultats d'expérimentation ou toute autre information en provenance d'autrui en le faisant passer pour sien ou sans en citer les sources;
- résumer ou paraphraser l'idée d'un auteur sans en indiquer la source;
- traduire en partie ou en totalité un texte en omettant d'en mentionner la source ou de le mettre entre guillemets ;
- utiliser le travail d'un autre et le présenter comme sien (et ce, même si cette personne a donné son accord);
- acheter un travail sur le Web ou ailleurs et le faire passer pour sien;
- utiliser sans autorisation le même travail pour deux activités différentes (autoplagiat).

Autrement dit : mentionnez vos sources

Document informatif V.3 (août 2017)