Université de Sherbrooke

Département d'informatique
IFT 814 – Cryptographie

Plan d'activité pédagogique
Automne 2024

Enseignants	Dave Touchette	Martin Fiset
Courriel :	Dave.Touchette@USherbrooke.ca	Martin.Fiset@USherbrooke.ca
Local :	D4-1018-2	
Téléphone :	+1 819 821-8000 x62847	
Disponibilités :	À déterminer en classe	

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

Horaire

Groupe 18 :	Exposé magistral :	Jeudi	18h30 à 21h20	salle D3-2034/Réunion Microsoft Teams
Groupe 28 :	Exposé magistral :	Vendredi	9h00 à 11h50	salle L1-2633
Groupe 51 :	Exposé magistral :	Jeudi	18h30 à 21h20	salle D3-2034/Réunion Microsoft Teams

Description officielle de l'activité pédagogique[1]

Cibles de formation :	Connaître les fondements théoriques et être capable d'utiliser correctement les principaux systèmes cryptographiques modernes. Connaître diverses applications de la cryptographie moderne, en particulier pour sécuriser l'information sur les réseaux. Obtenir un aperçu de diverses applications théoriques avancées de la cryptographie.
Contenu :	Cryptographie classique et moderne. Systèmes à clés privées et à clés publiques. Signature électronique et distribution de clés. Génération pseudo-aléatoire, fonctions de hachage, fonctions à sens unique et portes cachées. Implémentations pratiques. Confidentialité, authentification, identification, intégrité. Lancement de pièce de monnaie, mise-en-gage, transfert à l'aveugle, preuves à divulgation nulle et partage de secret. Introduction au calcul sécuritaire multipartite, à la théorie de l'information et à la cryptographie quantique.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Particularités	Aucune

[1] https://www.usherbrooke.ca/admission/fiches-cours/ift814

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

La cryptographie a débuté comme l'art d'encoder un message pour le transmettre de façon secrète, même s'il est intercepté en cours de route. La guerre entre créateurs de codes et briseurs de codes fait rage depuis des millénaires, mais c'est seulement dans les dernières décennies que la notion de sécurité cryptographique a été mise sur de solides fondations. En plus de discuter de confidentialité parfaite, la cryptographie moderne s'est étendue pour parler de notions d'intégrité de transmission et d'authentification de messages, en offrant une sécurité basée sur des problèmes calculatoires difficiles et des garanties contre des adversaires ayant un temps de calcul borné. Les relaxations étudiées permettent d'accomplir des tâches qui a priori pourraient sembler impossibles, tel qu'un protocole permettant à deux personnes ne partageant pas de secret préalable et discutant dans une salle bondée d'adversaires de s'échanger un message en toute confiance. Nous verrons que toutes ces primitives cryptographiques sont à la base de la sécurité de la communication sur internet et qu'ils sont également appliqués dans divers autres contextes. Nous survolerons également divers sujets de pointe en cryptographie comme le calcul sécuritaire multipartite, les preuves à divulgation nulle ainsi que la cryptographie quantique.

1.2 Cibles de formation spécifiques

À la fin de cette activité pédagogique, une étudiante ou un étudiant doit être capable :

1. de comprendre et savoir manipuler les principaux objets et concepts rencontrés en cryptographie, soit :
2. les systèmes de chiffrement symétriques et asymétriques
3. les codes d'authentification de messages
4. les protocoles interactifs d'échange de clés
5. les signatures numériques
6. les certificats numériques
7. les fonctions de hachage cryptographiques
8. d'intégrer ces diverses composantes en pratique dans une infrastructure à clé publique dans un contexte de sécurité de la communication sur les réseaux
9. de déterminer quels systèmes cryptographiques appliquer pour diverses situations informatiques
10. de manipuler les définitions de sécurité et d'évaluer la sécurité potentielle d'un système pour une situation donnée
11. d'être familier avec diverses notions avancées de cryptographie

1.3 Contenu détaillé

Thème	Contenu	Nbr. d'heures	Objectifs	Travaux
1	Introduction à la cryptographie : • Historique • Masque jetable et chiffrement parfait • Rappel de probabilités • Limite du chiffrement parfait • Sécurité calculatoire	7	1, 2, 3, 4	✔
2	Cryptographie symétrique : • Chiffrement symétrique • Codes d'authentification de messages • Définitions de sécurité • Constructions théoriques et pratiques	7	1, 2, 3, 4	✔
3	Cryptographie asymétrique : • Rappel d'arithmétique modulaire • Échange interactif de clé • Chiffrement asymétrique • Signatures numériques • Définitions de sécurité • Constructions théoriques et pratiques	7	1, 2, 3, 4	✔
4	Infrastructure à clé publique : • Notion de confiance • Certificats • Gestion de clés	3	1, 2, 3, 4	✔
5	Sujets avancés en cryptographie	12	5	✔

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 comporte trois heures de cours magistral. Durant les séances magistrales (typiquement au tableau à craie ou avec des transparents), la personne enseignante introduit des concepts ; énonce (et démontre) des résultats théoriques ; donne des exemples, etc.

2.2 Calendrier

Semaine	Date	Thème
1	2024-08-26	Activités étudiantes
2	2024-09-02	1
3	2024-09-09	1 et 2
4	2024-09-16	1 et 2
5	2024-09-23	2 et 3
6	2024-09-30	3
7	2024-10-07	3
8	2024-10-14	Examen périodique
9	2024-10-21	Relâche
10	2024-10-28	3
11	2024-11-04	3 et 4
12	2024-11-11	4 et 5
13	2024-11-18	5
14	2024-11-25	5
15	2024-12-02	Révision et 5
16	2024-12-09	Examen final
17	2024-12-16	Examen final

2.3 Évaluation

Devoirs (5)	60 %
Examen final	40 %

L'évaluation consiste en cinq devoirs et un examen final. Une pénalité de 33.4% par jour de retard sera appliquée aux devoirs. Les devoirs et les examens portent sur des questions théoriques en lien avec les thèmes du cours.

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

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 devoirs sont approximativement les suivantes : 20 septembre, 4 octobre, 18 octobre, 22 novembre, 6 décembre

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 le contenu du cours

4 Références

[1] A.J. MENEZES AND P.C. VAN OORSCHOT AND S.A. VANSTONE : *Handbook of Applied Cryptography*. CRC, 2001.

[2] J. KATZ AND Y. LINDELL : *Introduction to Modern Cryptography*. CRC, 2008.

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

[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/

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)