IFT6180–Cryptographie: Théorie et Applications (Plan de cours –hiver 2019)

Louis Salvail[1]

Université de Montréal (DIRO), Québec,
salvail@iro.umontreal.ca
Bureau: Pavillon André-Aisenstadt, #3369

1 Quand et où

Le cours aura lieu au rythme de deux périodes de 90 minutes par semaine. Les exercices seront donnés sous forme de devoir. Nous discuterons des solutions en cours.

Lundi 11:30-13:30 ⇒ B-3245, pav. 3200 J.-Brillant.
Mercredi 12:30-14:30 ⇒ local S-144, pav. Roger-Gaudry.

Le premier cours aura lieu le lundi 7 janvier 2019.

2 Matériel et Prérequis

Le livre suivant est très très très très très fortement suggéré:

Introduction to Modern Cryptography
Jonathan Katz
Yehuda Lindell
Chapman and Hall/CRC
Taylor and Francis Group

Le cours suivra ce livre de près. Un autre livre utile qui traite aussi des sujets du cours est:

Cryptography: Theory and Practice
(Discrete Mathematics and Its Applications)
Douglas R. Stinson
Chapman and Hall/CRC

Il existe une version française, traduite par Serge Vaudenay, du livre de Stinson.

Ce cours s'adresse aux étudiants avec une bonne connaissance des mathématiques discrètes. La connaissance des principes de bases de l'informatique théorique comme la complexité du calcul est un atout, en particulier les réductions polynomiales. Ce cours traite de la cryptographie d'un point de vue essentiellement théorique et n'abordera pas la sécurité informatique comme telle. Il est au sujet de la confidentialité et de l'intégrité de l'information au sens traditionnel. Ainsi, nous nous concentrons sur les méthodes de chiffrement, les codes d'authentification et les signatures numériques.

Le cours sera accompagné d'un site web:

www.iro.umontreal.ca/~salvail/crypto/index.html .

3 Plan

Le cours traitera des sujets suivants dans l'ordre approximatif indiqué ci-dessous. Les sujets étudiés suivront d'assez près le traitement du livre.

- Cryptographie symétrique
  1. Introduction
  2. Chiffrement parfait
  3. Chiffrement à clé privée et génération pseudo-aléatoire
  4. Codes d'authentification de message et fonctions de hachage résistantes aux collisions
  5. Chiffrement à clé privée dans la pratique
- Cryptographie asymétrique
  1. Théorie des nombres et hypothèses calculatoires
  2. Infrastructures à clés publiques
  3. Chiffrement à clé publique
  4. Signatures numériques
  5. Sécurité dans le modèle de l'oracle aléatoire
- Un peu de cryptographie quantique (si le temps le permet).

4 Évaluation

L'évaluation du cours se fera en deux parties:

1. Environ 5 devoirs dont au moins 3 doivent être faits individuellement. (60%)
2. Une présentation d'un article scientifique sur un sujet traité pendant le cours et choisi parmi une liste. La présentation sera donnée à toute la classe. La présence des étudiants aux présentations est requise. (40%)

La date prévue pour la première séance de présentations est 11:30-13:30 le lundi 15 avril 2019. D'autres périodes seront peut-être nécessaires pour l'ensemble des présentations.