# IFT6180–Cryptographie: Théorie et Applications (Plan de cours –Automne 2016)

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.

**Lundi 10:30-12:30** $\Rightarrow$ Z-205.
**Mardi 14:30-16:30** $\Rightarrow$ A.-A. 1411.

Le premier cours aura lieu le mardi 6 septembre 2016.

## 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 très 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. Le concept de *réduction* en informatique théorique est central dans le traitement que nous ferons de la cryptographie moderne. Ce cours traite de la cryptographie d'un point de vue essentiellement théorique et n'abordera pas la sécurité informatique comme telle. 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

## 4 Évaluation

L'évaluation du cours se fera en deux parties:

1. Environ $n \approx 5$ devoirs. (65%)
2. Un examen final sous forme d'une présentation sur un sujet parmi une liste de sujets proposés. (35%)