UQAC
UNIVERSITÉ DU QUÉBEC
À CHICOUTIMI

8INF854 – Cryptographie

Plan de Cours

Description sommaire

Historique: Notions élémentaires de la théorie des nombres et de la théorie de la complexité; Cryptologie à clef privée et publique; Signature électronique, fonctions de hachage à sens unique; Protocole d'échange de clefs, échange de clefs; Exemples de librairie dans des langages tels que C et Python; cryptologie quantique (si le temps le permet), Cryptosystèmes à courbes elliptiques (si le temps le permet).Le cours sera accompagné d'un site web:

Objectifs

Comprendre le fonctionnement des principaux protocoles et algorithmes cryptographiques ainsi que leurs applications.

Sommaire du cours

Le plan suivant donne un **aperçu** des sujets traités dans ce cours. Bien que nous allons essayer de respecter l'ordre indiqué ci-dessous, celui-ci ainsi que les contenus présentés **peuvent changer** en fonction des besoins. La plupart du temps une heure du cours du vendredi sera consacrée à la résolution d'exercices.

Préliminaires

- Présentation du cours, des objectifs, du syllabus

Introduction

- concepts de bases
- histoire de la cryptographie
  - Période artisanale (préhistoire)
  - Période mécanique
- Période scientifique

Mathématiques pour la cryptographie

- théorie des nombres
- complexité, ordres de grandeur
- Congruence
- algorithme d'Euclide, Euclide Étendu
- Inverse multiplicatif
- méthodes binaires
- représentations signées de l'exposant

Cryptographie classique

- Cryptographie mono-alphabétique : Chiffrement affine, chiffrement par substitution, carré de Polybe.
- Cryptographie poly-alphabétique : Chiffrement par permutation, chiffrement de Vigenere, chiffrement de Verman,
- Cryptographie poly-grammiques : chiffrement de Playfair, chiffrement de Hill…
- Cryptographie homophonique : le carré de 25 à représentations multiples, le renversement des fréquences, le système du dictionnaire
- Cryptographie tomogrammiques : chiffrement de Chase, chiffrement de Collon, chiffrement ADFGX