MAT3505/MAT3545 : Introduction à la cryptographie

Plan de cours

Professeur : Frédéric Rochon

Courriel : rochon.frederic@uqam.ca
Disponibilités : Prendre rendez-vous par courriel

Cours : Lundi et mardi de 13h30 à 15h
Page web : www.cirget.uqam.ca/rochon/enseignement/MAT3505-3545

Objectif du cours : Présenter la cryptographie et les principes mathématiques sous-jacents.

Préalables académiques :
MAT3505 : Avoir complété 54 crédits du programme ;
MAT3545 : MAT1060-Mathématiques algorithmiques ou INF1132-Mathématiques pour l'informatique.

Évaluation :

Outils d'évaluation	Dates	Pondération
Devoir I	29 septembre 2026	10%
Examen de mi-session	20 Octobre 2026	40 %
Devoir II	24 novembre 2026	10%
Examen final	15 décembre 2026	40%

Contenu du cours :

1. Les débuts de la cryptographie
2. Quelques cryptosystèmes simples
3. Cryptanalyse des systèmes classiques
4. Probabilités et théorie de l'information
5. Éléments de théorie des nombres
6. Cryptographie à clé publique
7. Cryptographie quantique
8. Informatique quantique et téléportation

Référence principale : La cryptographie de l'Antiquité à Internet, par François Bergeron et Alain Goupil, disponible en ligne.

Autres références :

— *Elementary Number Theory, Cryptography and Codes*, par M.W. Baldoni, C. Ciliberto et G.M. Piacentini Cattaneo ;
— *Introduction to cryptography*, par H. Delfs et H. Knebl ;
— *Cryptographie Théorie et pratique*, par Douglas Stinson.