Cryptographie algébrique (40 h, 6 ECTS)

Enseignant : Prof. D. Tieudjo

Objectifs

L'objectif du cours est de présenter **les concepts de base de la cryptographie, et les outils algébriques (surtout arithmétiques)** nécessaires pour la mise en œuvre des mécanismes et systèmes de la cryptologie moderne, tant en ce qui concerne la cryptographie conventionnelle que les méthodes à clé publique. Les procédés cryptographiques étudiés sont reliés aux fonctionnalités qu'ils assurent, en termes de sécurité : confidentialité, intégrité, authentification, chiffrement, signature, …

Plan du cours pour 2011

Le cours est découpé en 8 chapitres : 6 des 8 chapitres seront examinées en cours et 2 chapitres (parties) sont réservés en TPE.

1. Introduction à la cryptologie ;
2. Groupes, anneaux et corps : applications aux anneaux des entiers et polynômes et utilisation en cryptologie ;
3. Arithmétique et algorithmique des entiers et des polynômes : tests de primalité, factorisation, problème du logarithme discret, résidus quadratiques et symboles de Legendre et de Jacobi ;
4. Cryptographie symétrique ;
5. Cryptographie asymétrique : étude des quelques schémas cryptographiques :
   - Schémas de chiffrement : RSA, Rabin, El Gamal,
   - Protocole d'échange DH,
   - schémas d'authentification et signature ;
6. Fonctions de hachage ;
7. Cryptanalyse de certains schémas : RSA, El Gamal, DH, schémas d'authentification et signature.
8. Principaux domaines d'application.

Place du cours dans le programme de Master

Pré-requis

Un minimum de connaissance en algèbre (structures algébriques, algèbre linéaire, arithmétique) et en probabilité est requis. Les outils algorithmiques de base doivent être maîtrisés. Des notions de complexité d'algorithmes et de la théorie de l'information sont également nécessaires.

Langue

Le cours sera donné en français (une documentation en anglais est disponible).

Bibliographie

- F. Arnault, *Théorie des nombres et cryptographie*, Cours de DEA, Université de Limoges (2002)
- A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press. (1996)
- J. Rosenthal, *Cryptography*, Winter course term, University of Zurich (2004/05)
- H. Schauer, *Introduction à la cryptographie*, Support de cours, Cabinet Hervé Schauer Consultants (2001)
- D. Stinson, *Cryptography: Theory and Practice*, CRC Press. (1995)