Introduction à la Cryptologie

Chapitre 1 : Introduction et présentation du cours

Michael Eisermann (Institut Fourier, UJF Grenoble)

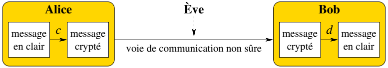
Année 2008-2009

IF / IMAG, Master 1, S1-S2

document mis à jour le 7 juillet 2009

www-fourier.ujf-grenoble.fr/~eiserm/cours # crypto

Cryptologie = «science du secret »



La cryptologie englobe deux approches complémentaires :

- Cryptographie = «écriture secrète »
  - transformer message clair en message chiffré
  - étude et conception des procédés de chiffrement
- Cryptanalyse = «analyse de cryptogrammes »
  - techniques pour déchiffrer des messages secrets
  - évaluation des faiblesses et des attaques possibles

Elle connaît maintes applications :

- communication sécurisée sur internet,
- cartes bancaires, monnaie électronique,
- authentification des documents électroniques,
- protection des droits d'auteur, . . .

Objectifs du cours

Outils nécessaires pour la cryptologie :

- Mathématiques !
- Informatique !

Objectifs du cours :

- Fondements mathématiques
- Fondements algorithmiques

$\Rightarrow$ Introduire à la cryptographie à clé secrète et à clé publique

Perspectives :

- Préparer au Master 2 Professionnalisant —
  Sécurité, cryptologie et codage de l'information
- Culture générale en math-info
- Oral de l'agreg

Organisation du cours

Module commun entre l'IMAG et l'IF.

Équipe pédagogique :

- Laurent Fousse (IMAG)
- Michael Eisermann (IF)

Enseignements : les vendredis 13h30–15h00 + 15h15–16h45

Volume horaire : 6 ECTS

- 1er semestre : $8 \times$ 3h cours/TD $+$ $2 \times$ 4h30 TP
- 2nd semestre : $8 \times$ 3h cours/TD $+$ $2 \times$ 4h30 TP

Total : $\approx$ 60h plus travail personnel

Un exemple en miniature

Considérons l'alphabet $\{\mathtt{A}, \mathtt{B}, \mathtt{C}, \dots, \mathtt{Z}\}$ et les deux permutations

$$c = \begin{bmatrix} \mathtt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \mathtt{XYZABCDEFGHIJKLMNOPQRSTUVW} \end{bmatrix},$$

$$d = \begin{bmatrix} \mathtt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \mathtt{DEFGHIJKLMNOPQRSTUVWXYZABC} \end{bmatrix}.$$

Ici le message	$m =$	`CECI EST UN MESSAGE`
est crypté en	$\bar{m} = m^c =$	`ZBZF BPQ RK JBPPXDB`
puis décrypté en	$m = \bar{m}^d =$	`CECI EST UN MESSAGE.`

Cryptanalyse : Ce cryptage alphabétique n'est pas du tout sûr !
Même avec des permutations plus compliquées. . . 26 est trop petit.

```
ERL BLCNEOGOJQR GFLGOQJCL LTO ER BLE BFET TECL NGJT OQEHQECT BGT
OCLT IECL G ILACXBOLC. PQET PLRLV IL DQECRJC FG BCLEPL. GPLA ER
BLE IL TOGOJTOJUEL LO ER IJAOJQRRGJCL DCGRAGJT ER BCQSCGNNL BLEO
FL DGJCL JRTOGROGRLNLRO.
```

Idée : utiliser l'alphabet $\{0, 1, 2, \dots, N-1\}$ où N est gigantesque.
Outils : arithmétique modulaire & algorithmes efficaces

Thèmes abordés

Aspects algorithmiques de la sécurité (Laurent Fousse)

1. Histoire des codes secrets
2. Complexité des algorithmes
3. Théorie de l'information, entropie
4. Chiffrement à clef secrète (DES, AES)
5. Hachage, intégrité, authentification
6. Codes correcteurs

Outils mathématiques pour la cryptographie (Michael Eisermann)

1. Arithmétique des entiers, aspects algorithmiques
2. Les entiers modulo n, aspects algorithmiques
3. Nombres premiers, cryptographie selon RSA
4. Le vocabulaire des groupes et des anneaux
5. Arithmétique des polynômes, aspects algorithmiques
6. Les corps finis, aspects algorithmiques

Pré-requis

Informatique :

- Langage de programmation (le C++, disons)
- Familiarité avec des notions d'algorithmique
- Ouverture d'esprit et la volonté d'apprendre

Mathématique :

- Langage et raisonnement mathématiques
- Calcul algébrique, algèbre linéaire, espaces vectoriels
- Ouverture d'esprit et la volonté d'apprendre

Littérature

Documents du cours :
`www-fourier.ujf-grenoble.fr/~eiserm/enseignement`

Pour réviser les notions de base on pourra consulter

- Bernard Ycart *et al* : *Maths en Ligne*,
  `http://ljk.imag.fr/membres/Bernard.Ycart/mel/`.
  (*structures algébriques*, *arithmétique*, *polynômes*)
- Nathan Jacobson : *Basic Algebra*,
  Freeman and Company, 1985.
- Roger Godement : *Cours d'algèbre*,
  Hermann, 1966.

Le présent cours n'est qu'une modeste introduction.
Voici quelques bouquins pour aller plus loin :

- Simon Singh : *Histoire des codes secrets*,
  LGF - Livre de Poche, 2001.
- Joachim von zur Gathen, Jürgen Gerhard :
  Modern Computer Algebra, Cambridge University Press, 1999.
- Donald E. Knuth : *The art of computer programming*,
  Addison Wesley, 1969.