Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 29 janvier 2010

Présents: Didier Alquié, Sandrine Blazy, Christophe Chabot (invité), Sylvain Duquesne, Mohamed El Belghiti, Lionel Fourquaux, Aurore Guillevic, Pierre Loidreau, David Lubicz (invité), Soline Renner.

Bilan du premier semestre de M1

- « Algorithmique de base (ALBA)»
  LF : résultats pas mauvais. Le programme a pas mal évolué: moins de théorie, plus d'aspects programmation de base. Grosse disparité de niveau en maths par rapport à l'an dernier. Nécessité d'un module de complément en mathématiques ?
  Coupure cryptographie/analyse numérique, tension au niveau des attentes.
  Ce serait mieux de faire d'abord « programmation C » pour pouvoir aborder sereinement les TP.
  MEB : problème de structure dans le cours, pour savoir ce qui est important.
  SD* : toutes les problématiques liées à la mutualisation avec l'analyse numérique ne se poseront plus ou du moins plus dans les mêmes termes puisqu'il est envisagé que cette spécialité quitte le master de maths pour créer un nouveau master de Modélisation et calcul scientifique avec les mécaniciens.
- « Algèbre de base »
  MEB : l'enseignant de TD n'était pas très satisfaisant et avait l'air de mal maitriser.
- « Théorie des nombres »
  MEB : bien mais quelques problèmes avec des TD visiblement insuffisamment préparés par l'enseignant.
- « Programmation C (ProgC)»
  CC : un peu court mais heureusement il y a les TP d'ALBA pour pratiquer.
  Projet en analyse pas bien adapté parce que l'intervenant n'est pas au courant de ce qui se fait dans le module (cf *).
  MEB : trop court. Il faudrait plus d'heures de cours voire passer le module à 6 ECTS. Problème d'étudiants qui ne suivent que ALBA et qui sont perdus en C → le rajouter dans la description du module ALBA. Projet d'analyse HS, pourquoi pas un projet au choix Algèbre ou Analyse (cf *)?
- « Probabilités et statistiques pour l'ingénieur (PSIN)»
  Encore trop peu de statistiques cette année malgré le changement d'enseignant et les remarques remontées par SD en septembre (cf *).
  MEB : les étudiants s'interrogent sur l'utilité des probabilités dans la formation ?
  DL : les probabilités/statistiques sont très présentes en cryptographie même si on a plutôt besoin de probabilités discrètes.
- « Anglais »
  MEB : bcp de travail pour petit coefficient et contenu trop éloigné de la formation.
  ?? : C'est important de le garder car très présent dans le monde professionnel. Pour ce qui est du contenu, les étudiants sont encouragés à utiliser les références en anglais proposées par les enseignants. Il est aussi remarqué qu'il faut communiquer la dessus lors des réunions de rentrée.
- Autres remarques
  MEB : Ce semestre reste général, et les étudiants ne découvrent pas la cryptographie. Les étudiants regrettent qu'il n'y ait pas de module de sport noté.
  SD/DL : Ce n'est pas le but de la formation de faire du sport. C'est très bien que les étudiants en fasse mais ça ne fait pas partie de la formation.
  LF: Essayer de rapprocher ALBA de ALGB ou de THNO car c'est un peu trop

indépendant. Par exemple via le projet de ProgC.

Bilan du premier semestre de M2

- « Mathématiques pour la cryptographie (MACR)»
  DL : Julien Sebag souhaite que le cours soit mieux coordonné avec le cours de M1 (résultants). Il a du transformer des heures de TD en heures de cours car il n'y a pas assez d'heures de cours. Il souhaiterait aussi plus d'interventions extérieures pour les parties algorithmiques (LLL, Groebner).
  AG/SR : pas assez d'heures de cours. Examen pas très clair du fait des nombreux intervenants.
  SD: ce dernier problème sera résolu l'an prochain par le passage de toutes les modalités de contrôle des connaissances à du contrôle continu uniquement.
- « Cryptographie avancée »
  AG/SR : passer plus de temps sur les couplages et sur les diviseurs. Homogénéiser plus avec MACR sur les courbes elliptiques de base.
  DL : manipuler les diviseurs avec magma pour mieux les approprier.
- « Programmation pour la cryptographie »
  AG/SR : il manque un peu rappel de cours de Java, comment on écrit les classes. Les étudiants ont eu du mal à cerner les attentes de l'enseignant et le système de notation. Les premiers cours/TP n'étaient pas assez proche de la cryptographie effectivement utilisée actuellement. L'examen (écrit) était en décalage par rapport à l'enseignement (TP).
  SD : ce dernier problème sera résolu par le passage au contrôle continu.
  PL : est il vraiment nécessaire d'avoir du C++ et du Java ? Une fois qu'on connait l'un, il est très facile de s'adapter.
  SD/DA: c'est quand même une bonne chose d'avoir pratiqué les 2 au moins pour le CV.
- « Systèmes d'exploitation, Réseaux informatiques, Sécurité »
  AG/SR : bien
- « Programmation objet, C++ »
  AG/SR : plus théorique que pratique.
  DL: voir la librairie NTL (LLL) en projet par exemple.
- « Environnement économique et juridique de l'entreprise »
  AG/SR : bien.
- « Sécurité des services en ligne »
  AG/SR : bien, mais les étudiants sont défavorisés en TP par rapports aux étudiants de SSI qui ont plus de pratique du C et semblent déjà bien connaître le sujet.
- « Protection de contenu »
  AG/SR : bien mais c'est un survol du sujet un peu trop superficiel. Problème d'emploi du temps avec l'anglais. Les étudiants de Supelec avaient des TD pour mettre en pratique le cours.
  SD/PL : rajouter des heures de TD spécifiques aux étudiants de maths (financement ?) ou des TP de tatouage.

AG/SR : Globalement, le premier semestre est un peu trop chargé et les étudiants ont rencontré des problèmes de disponibilité des livres à la bibliothèque de l'IRMAR. Les interventions de professionnels seraient plus bénéfiques si elles avaient lieu plus tôt dans l'année.
SD : On essaiera d'alléger l'an prochain. Le problème vient des modules mutualisés avec l'IFSIC/Supelec (SSL, Protection de contenu) qui ont ont lieu au premier semestre mais comptent pour le second. Pour les livres, il ne faut pas hésiter à demander à la bibliothécaire

ou à me le signaler pour en commander de nouveaux.

Point sur les stages

SD : Les offres de stage ont été assez nombreuses. Tous les étudiants sauf un ont déjà trouvé un stage.
AG/SR : Les étudiants aimeraient une réunion pour savoir ce qui est attendu du stage. Ils regrettent également que SD ait découragé certains étudiants de candidater sur les stages proposés par Marc Joye et Jean-Claude Carlach et surtout le manque de diplomatie. Du coup, ces étudiants ont été démotivés pour envoyer des candidatures sur tous les stages que SD leur a fait suivre de peur qu'il ne leur barre la route.
SD : Cela a été fait car SD voulait de bons étudiants pour ces stages à la demande des encadrants suscités. SD regrette de ne pas avoir présenté les choses plus habilement. Par contre il n'y a jamais eu, ni même intention d'avoir, de commentaires négatifs sur les étudiants en ce qui concerne les autres offres de stages. D'ailleurs, dans la grande majorité des cas, les responsables de stage ne demandent pas d'avis sur les étudiants. Il est dommage que les étudiants se soient sentis restreints dans leurs recherches de stage.

Mutualisation avec l'IFSIC

SD : SSL semble être plutôt une réussite. Il serait bien d'arriver à ouvrir eVote l'an prochain. Les modules optionnels de SSI peuvent avoir lieu jusqu'à fin janvier. Il est donc tout à fait possible que les étudiants de SSI choisissent « Cartes à puces » si celui ci est fait en Janvier comme cette année. Il faut donc rajouter cette option dans le parcours SSI.
SB : SSL risque de ne pas ouvrir l'an prochain car l'enseignant ne veut plus le faire. Les étudiants de SSI ne choisissent pas eVote car ils ont l'impression que ce module est redondant avec AUTH. Il faut donc revoir le résumé du module pour éviter cette confusion.

Page web sécurité commune avec l'IFSIC

SD présente un début de premier jet. L'idée est d'avoir une page assez simple jouant simplement le rôle de portail vers les sites propres des formations et expliquant les spécificités des 2 formations. Le principe convient à tout le monde et SD et SB s'occupent donc de finaliser la page au plus vite pour qu'elle soit opérationnelle quand les étudiants chercheront quoi faire l'an prochain.

Association des anciens étudiants

DL : L'université peut fournir l'hébergement du site et il est préférable que cette voie soit privilégiée. Il est nécessaire que l'association soit crée pour cela et les étudiants sont encouragés à faire les démarches le plus vite possible. DL insiste sur la simplicité de ces démarches.
Plusieurs intervenants insistent sur le fait que les étudiants ont beaucoup à gagner avec ce type d'association pour se créer un réseau de contacts même si, en tant que premiers, il faut la créer. Le président de l'association n'a pas vocation à y rester à vie. Des mandats de 3 ans peuvent être envisagés.

Page Web de la formation

PL présente un texte de présentation du master. Ce texte est joint en annexe à ce compte rendu et tous les commentaires sont les bienvenus.

Modification des parcours pour 2010-2011

SD va faire la demande pour faire quelques changements dans les parcours

- Echange de « spécialisation en cryptographie 1 (S4)» et « Environnement économique et juridique de l'entreprise (S3)» puisque c'est ce qui se passe effectivement en pratique.
- Laisser ODRO et Logique au choix en S2 au lieu d'imposer ODRO.
- Suppression de Automates et Complexité en S4 puisqu'il n' plus de raison d'être à cause de la modification précédente (il s'agit en fait de la moitié du module de logique)
- Passage de toutes les modalités de connaissances en CC pour le M2.

Formation à la rédaction de CV, lettre de motivation, entretien

Les étudiants ont accès aux services du SOIE qui semblent être très satisfaisants. L'an prochain SD s'occupe de leur demander la création d'un atelier spécifique au Master.
PL rappelle les bases pour un CV et une lettre de motivation : CV sur une page et lettre de motivation véritablement spécifique à l'entreprise visée (sans pour autant être exagérément flatteuse).

Annexe : proposition de PL pour la présentation du Master sur la page web

Le Master *Mathématiques de l'information, Cryptographie* forme des ingénieur-experts, spécialisés dans le domaine de la protection de l'information numérique.

Parmi les secteurs économiques à forte croissance et créateur d'emplois se trouvent les deux principaux secteurs complémentaires concernés par cette formation : Le secteur de l'informatique et celui des communications numériques. En témoignent le très fort développement de la téléphonie mobile, des réseaux sans fils, des transactions à distance par internet, l'utilisation généralisée de cartes à puces dans la sécurisation des transactions commerciales, les techniques d'identification biométriques, l'identification à distance (RFID par exemple),...

Comme l'information numérique transitant entre deux points est susceptible d'emprunter de multiples voies (satellitaires, antennaires, par fibre optique, par liaison filaire, par courant électrique,...) son intégrité, voire sa confidentialité, se doivent donc d'être protégées tant contre des perturbations naturelles dues au canal de transmission (domaine de la correction d'erreurs) que contre des attaques malveillantes (domaine de la cryptologie).

Les fondements mathématiques de la modélisation et le traitement de l'information numérique font intervenir plusieurs branches des mathématiques comme l'Algèbre, la Géométrie, la Combinatoire, les Probabilités. En outre la mise en oeuvre d'une infrastructure de protection de l'information s'appuie sur une bonne connaissance des systèmes d'exploitation, des réseaux ainsi que de la programmation.

Etre spécialiste de la protection de l'information signifie donc faire preuve d'éclectisme : D'une part il faut maîtriser des mathématiques complexes mises en jeu tant du point de vue théorique que du point de vue algorithmique. D'autre part il est indispensable de pouvoir les mettre en oeuvre dans des infrastructures très diverses. C'est l'objectif du Master.

Cette formation s'inscrit dans le cadre d'un partenariat entre l'institut de mathématiques de Rennes (IRMAR) et le laboratoire de cryptographie du Celar qui est en charge de la conception d'algorithmes cryptographiques gouvernementaux.