Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 21 Février 2014

Présents: Delphine Boucher, Xavier Caruso, Sylvain Duquesne, Pierre-Alain Fouque, Pierre Loidreau, Antoine Loiseau (M2), Julien Proy (M1), Christophe Ritzenthaler (via Skype)

Bilan des cours de M2

- « Courbes algébriques »
  AL : pas assez d'heures essentiellement parce que ça va trop vite ou alors plus de TD. SD et CR vont rediscuter le contenu de ce cours afin de mieux l'adapter au volume horaire.
- « Théorie algorithmique des nombres pour la cryptographie »
  AL : Emploi du temps trop serré. Pas assez de prérequis sur les corps finis.
  Une discussion s'engage (faisant suite à une discussion électronique préalable sur le même thème). Il en ressort
  1. Le problème se situe au niveau d'un manque de pratique de manipulation des corps finis.
  2. Le contenu des différents cours introduisant les corps finis (ALGB, THNO, COCO) est suffisant.
  3. Les étudiants doivent travailler par eux mêmes entre le M1 et le M2 pour se mettre à niveau sur leurs lacunes de M1 et notamment en faisant des exercices sur les corps finis si ils ne s'y sentent pas à l'aise. Les pages web de toutes les formations de l'UFR de maths sont en train d'être actualisées pour qu'une référence bibliographique soit indiquée pour chaque module.
  4. En fait les problèmes semblent surtout porter sur les corps p-adiques et corps de fonctions ce qui est nettement moins inquiétant et moins étonnant.
- « Cryptographie avancée »
  AL : pas de retours particuliers en dehors des problèmes d'emploi du temps
- « Architecture, Systèmes, Réseaux »
  AL/JP : l'intervenant n'a pas plu. Étude des produits CISCO. Que du réseau et pour spécialiste. A la limite utile pour des admin réseau mais pas pour des cryptographes. Pas appris/compris grand chose.
  SD : Ça a été très difficile de trouver un intervenant. On tachera de trouver mieux l'an prochain. PL précise que des gens de la DGA doivent pouvoir faire ce genre de cours.
- « Programmation 1 (Java) »
  AL : les TP orienté crypto c'est bien. Problème de personne avec l'intervenant. Module trop peu orienté objet.
  Ce serait mieux de d'avoir un cours de C++ de 6 crédits et un cours de Java de 3 crédits
  SD : pas si simple car ce sont des modules mutualisés.
  PL : Pourquoi ne pas faire qu'un seul langage objet (du C++).
  SD/PAF : Le java est indispensable en entreprise
  JP : Aucun retour en M1.
- « Cryptographie Quantique »
  AL :La crypto n'apparaît que dans le dernier cours sinon c'est que des espaces de Hilbert, il faudrait que ça vienne un peu plus tôt. Pas de q-bit et il manque la correspondance avec la physique quantique. Pourquoi ce module est il obligatoire.
  SD : il ne le sera plus l'an prochain et je ferais remonter la demander de faire plus de crypto et moins de maths.
- « Sécurité des Réseaux Informatiques »
  AL :un peu fourre tout (plein d'intervenants). Profs étonnés de voir des étudiants de

crypto. Manques en réseau.
PAF : On préviendra les intervenants l'an prochain.
Les problèmes étaient surtout pour IPSEC/VPN mais pour d'autres groupes d'info aussi.

- « Technique de recherche d'emploi »
  AL : TB. Pas grand chose en cryptographie au forum
- « Anglais »
  AL : Groupes de niveau mais très mal faits. Au niveau du contenu ça dépend des intervenants. Prépa au CLES très limitée.

Options

- « C++, les bases »
  AL : vraiment bien, arrêté un peu tôt. Ça aurait été bien de pouvoir aller plus loin.
- « Protection de contenu »
  AL : Bien pour la culture générale, à prendre en surnuméraire
- « Protection de la vie privée »
  AL : retour très contrastés
- « Auth »
  AL :beaucoup de déjà vu
  PAF : Idem en SSI, ça va évoluer
- « programmation parallèle, GPU »
  AL : TB
- « IDS »
  AL :TB très intéressant mais difficile

Globalement
AL : emploi du temps désordonné
SD : C'était clairement loin d'être idéal et dû à des contraintes exceptionnelles des intervenants. Je regrette également mais je n'ai pas pu faire mieux.

Point sur les stages

Pris par le temps, on a complètement oublié de parler de ce point, pourtant important car plusieurs étudiants n'ont pas encore trouvé de stage.

Bilan du premier semestre de M1

- « Algorithmique de base »
  JP :Assez difficile mais ça a plu. Peu de retours.
- « Algèbre de base »
  JP :Plutôt difficile mais peu de retours
- « Programmation scientifique 1 »
  JP :trop axé modélisation et pas de crypto. Façon surprenante de noter les TP. Mais quand même appris à programmer.
  PL : il y a quand même des fonctions qui servent en crypto et pas en analyse (eg >>)
  SD : Le cours est généraliste et ces fonctions sont vues (JP confirme). Par contre les TP sont basés sur l'analyse numérique mais (même si c'est moins motivant) ce n'est pas très important. Prévenir au début de l'année.
- « Probabilités pour la théorie de l'information»
  JP : OK

- « Réussir son insertion professionnelle »
  JP : OK mais intervenant généraliste sur l'insertion et ne connaît pas le milieu et les débouchés crypto.
- « Anglais »
  oublié (décidément...)

Globalement
JP : les tiers temps doivent être pris en compte de façon plus respectueuse (impossible de travailler au début ou à la fin du temps officiel quand les autres étudiants arrivent/partent, surtout quand ils arrivent)
SD/DB/XC : c'est noté mais c'est vrai que ce n'est pas simple à organiser.

Association des anciens étudiants

Comme les années précédentes, l'association survit difficilement car personne ne veut y consacrer du temps. La page facebook semble cependant bien vivante et il faut relancer l'idée d'avoir un mail de redirection d'anciens du type prenom.nom@crypto-rennes.org à défaut d'avoir prenom.nom@univ-rennes1.org que l'université ne veut pas mettre en place (mais il faut demander à la fondation rennes1). SD va relancer la fondation et en cas de réponse négative ou nulle va voir avec l'UFR de maths si elle peut héberger ça.