Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 14 janvier 2011

Présents: Didier Alquié, Sandrine Blazy, Antoine Chambert-Loir, Sylvain Duquesne, Mohamed El Belghiti, Pierre Loidreau, Marie-Alice Lossois, Anna Morra (invitée), Victor Servant (invité).

Bilan du premier semestre de M2

- « Mathématiques pour la cryptographie »
  SD : La répartition horaire a été changée par rapport à l'an dernier. Julien Sebag est plutôt satisfait de ce qui a été fait cette année.
  VS : Les étudiants aimeraient plus d'heures de cours pour le même programme. Ils souhaiteraient également commencer plus tôt ce cours et qu'il y ait un plus grand décalage temporel entre ce cours et crypto avancée. Un TP supplémentaire sur Schoof serait également le bienvenu.
  SD : Il est difficile de donner plus d'heure. On peut éventuellement transformer des heures de TD en heures de cours mais il n'est pas sûr que ce soit bénéfique. Par contre, on peut décaler sans trop de problème le cours de crypto avancée.
- « Cryptographie avancée »
  MEB : Quelques difficultés, notamment sur les couplages.
  SD : Difficile d'avoir une dynamique du groupe. Les étudiants posent trop peu de questions, d'autant plus si des parties du cours sont mal comprises comme les couplages.
  VS : Un TP supplémentaire encadré sur les attaques statistiques aurait été bien
- « Programmation pour la cryptographie »
  VS : Il manque un petit cours de java au début pour expliquer la syntaxe, par exemple en commencant par un TP simple. Pas nécessaire en ce qui concerne la manipulation des classes car c'est fait en C++. Par contre arbre, etc c'est inutile car ca a été fait en ALBA. De l'aritmétique sur les corps finis serait plus utile que des arbres ou de la stegano.
  SD : Décaler un peu le cours par rapport au cours de C++ pour avoir de l'avance sur les classes.
  ACL : On peut envisager un tutoriel Java en autonomie avant le début du cours
- « Systèmes d'exploitation, Réseaux informatiques, Sécurité »
  VS : pas mal. Rapport de TP inutiles pour le prof et les étudiants parce que les TP sont très précis et ils ne savent pas faire un rapport de TP. Les étudiants ont du mal à cerner ce qu'on attend d'eux à l'exam (il faudrait plus de TD). Vu le travail demandé pour les TP, ce serait bien que la note de TP ait plus d'importance dans la note finale. Ce serait bien qu'il y ait plus de SSL ou de choses liées à la sécurité.
  SD : Le dernier point est du au fait que le module SSL n'a pas ouvert cette année.
  PL/DA : important de commenter son codes et les rapports de TP sont un bon début.
  SD : il doit expliquer ce qu'il attend exactement dans ces rapports. I
- « Programmation objet, C++ »
  MEB/VS : TB
- « Technique de recherche d'emploi » et plus généralement rôle du SOIE
  SD : Contrairement à l'an passé, il y avait un module spécifique de 10h cette année. Les étudiants avaient bien sûr toujours accès aux services du SOIE (aide personnalisée pour les CV, lettres de motivations, ...)
  VS : TB mais étaler un peu plus.
- « Anglais »
  SD : Assez tendu, notamment en raison de problème d'emploi du temps avec les

modules d'informatique (PC par exemple). On essaiera de mettre les étudiants dans un groupe d'info l'an prochain.
MEB/ACL : inutile pour les bons et les mauvais
Discussion globale : il faut chercher l'anglais ailleurs qu'au SCELVA seulement car ils font ce qu'ils peuvent avec les moyens du bord.

- Projet de M1 en angleterre, Pays-Bas ou Allemagne, il y a surement de l'argent à l'univ pour ca ou
- Voire même petits boulots d'été.
- Faire parler les prof invités (4h chacun par exemple).
- Les étudiants doivent se forcer à lire les livres scientifiques en anglais.

- « Protection de contenu »
  SD : Moitié de cours du Master recherche en informatique. Comme évoqué l'an dernier lors de ce même comité, un cours/TD de 3h a été rajouté par rapport à l'an dernier et des TP seront rajoutés l'an prochain.
  VS : Manque du traitement du signal. Encore trop superficiel.
- « Contôle d'accès »
  VS : bien mais pas de TP
  SD/SB : c'est normal car le cours n'a ouvert qu'en Master Recherche et pas en SSI (qui rajoute habituellement des TP) faute d'étudiants.
- « Detection d'intrusion »
  VS : Assez inapproprié pour les étudiants; ils rament pas mal.
  SB : C'est normal c'est un cours assez bas niveau
- « Protection de la vie privée »
  MEB : TB

  Globalement les étudiants s'adaptent bien aux différents langages de programmation et semblent mieux préparés que l'an dernier de ce point de vue.

Mutualisation avec l'IFSIC

SD : Des modules n'ont pas ouvert cette année pour des raisons d'effectifs. Pour éviter que trop de modules de SSI ne ferment, « Cartes à puces » ne leur a pas été proposé.
SB : Ca devrait aller mieux l'an prochain

Point sur les stages

SD : 5 des 8 étudiants ont déjà trouvé un stage. Comme évoqué l'an dernier lors du comité, une réunion sera organisée en février pour savoir ce qui est attendu du stage.
VS : Pas assez de connaissance en début d'année pour savoir si un stage les concerne ou pas (crypto basée sur l'identité, canaux cachés)

Association des anciens étudiants

SD : Les étudiants de l'an dernier ont crée l'association mais ne sont pas allés plus loin faute de temps. Comme il a été dit l'an dernier les étudiants ont beaucoup à gagner avec ce type d'association pour se créer un réseau de contacts. Ils faudrait que les étudiants de cette année fasse une page web, même très simple avec au moins un annuaire qui puisse être facilement mis à jour. Ce serait bien de désigner une ou 2 personnes pour çà.
ACL : C'est pas très compliqué surtout l'université héberge.
Les étudiants ne connaissent pas forcément les outils (Php, sql) mais c'est pas compliqué vu ce qu'ils savent déjà faire, c'est une excellente occasion d'apprendre et pendant leur stage, ils seront en contact avec des gens qui savent faire.

Paiement des intervenants extérieurs

SD : L'an dernier, le paiement a été très difficile et aura mis quasiment un an. Pour éviter que ca ne recommence, les dossiers doivent être remis dès le mois de Janvier, même si les interventions n'ont pas encore eu lieu.

Bilan du premier semestre de M1

- « Algorithmique de base »
  ACL : content, note correctes donc le barème est resté sur 20 contrairement à d'habitude.
  MAL: pas contents de leurs notes. Cours bien par rapport à l'an dernier.
- « Algèbre de base »
  MAL: Cours dur mais bien expliqué et clair. Par contre TD pas terrible.
- « Théorie des nombres »
  MAL: pas assez structuré. Pas fait dans l'ordre. Problème des magistériens qui suivent les mêmes cours mais ont un bien meilleur niveau.
  ACL : Il faut faire le programme qui a été décidé par l'UFR. Ca a déjà été signalé à l'intervenant
- « Programmation C »
  AM : Groupe très hétérogène.
  MAL: le 1er TP était trop dur. Les commandes de base ce serait mieux. Après ca va beaucoup mieux. Module trop court.
- « Probabilités et statistiques pour l'ingénieur (PSIN)»
  MAL: Toujours aussi inadapté et cette année ils n'ont même pas fait les tests statistiques.
  SD : Ces 2 modules seront modifiés en conséquence dans la prochaine habilitation (ie à partir de 2012).
- « Anglais »
  MAL: organisation mieux (étalé sur l'année)
  SD: proposition de faire les projets tutorés en anglais pour forcer les étudiants à utiliser une biblio en anglais