Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 2 Mars 2014

Présents: Delphine Boucher, Xavier Caruso, Sylvain Duquesne, Pierre-Alain Fouque, Pierre Loidreau, Julien Proy (M2), Christophe Ritzenthaler, Michael Sagliano (M1).

Bilan des cours de M2

- « Courbes algébriques » et « Théorie algorithmique des nombres pour la cryptographie »
  JP : ça a plu dans l'ensemble, c'est dommage qu'il n'y ait qu'une seule note par module.
  CR : ce sont des petits modules qui doivent être vu comme complémentaires . Ça a peu de sens de faire une évaluation au bout de 6h de cours. Est ce que les TP ont été utiles ?
  JP : oui et ça passe bien, pas de soucis sur les aspects programmation peut etre ce serait l'occasion d'avoir une note.
  SD, DB : c'est pénible de noter.
  CR va réfléchir à une seconde note.
- « Théorie des nombres »
  JP : Le cours a bien plu. C'est bien de le faire en M2 plutôt qu'en M1.
- « Cryptographie avancée »
  JP : pas de retours particuliers, ça a plu. Examen plus dur que les années précédentes. Le cours et les TP sur la partie symétrique étaient bien mais l'examen est mal passé.
  SD, PAF : préparé un peu en dernière minute. On verra à rallonger l'an prochain ou faire un sujet plus simple.
- « Programmation 1 (Java) »
  JP : bien dans l'ensemble. Beaucoup de TP crypto. Mais l'intervenant considère que les étudiants ont a déjà des bases en java.
  MS : beaucoup de TP, c'est bien mais pas homogène. Il faudrait que ce soit un peu mieux réparti.
  SD : les prérequis en java sont un problème récurrent de ce module. Il a été plus ou moins résolu en M2 par les devoirs de vacances, mais ça ne fonctionne pas pour le M1. Une information à ce propos sera donnée l'an prochain.
- « Cryptographie Quantique »
  JP : pas beaucoup de crypto, peu de quantique, bref un peu trop maths.
- C++
  JP : très bien. Ce serait bien de pouvoir continuer avec la seconde partie de ce cours.
  SD : La seconde partie est très orientée vers le numérique. C'est pour ça qu'elle n'est pas proposée.
- « Sécurité des Réseaux Informatiques »
  JP : beaucoup de choses différentes et toujours pas assez de bases en réseau. un peu fourre tout (plein d'intervenants). Surtout pour les TP (le crypto de chaque trinôme ne fait rien). Partiel trop tard (3 mois après les cours),
  PAF : il faut rajouter une mini introduction pour chaque intervenant au moins pour que le cours apporte des choses. Il faut aussi prévenir les étudiants que les TP c'est pas grave si ils sont en observation. Changer les MCC en enlevant la note de TP.
  CR : proposer quelques cours de mise à niveau
  SD : difficile à faire financièrement parlant, par contre fournir des documents ou des introductions à étudier en amont du cours est une bonne idée. Et normalement le cours d'ASR a été mieux fait cette année que l'an dernier. On devrait finir par converger vers quelque chose d'acceptable même si ce ne peut pas être parfait puisque ce cours s'adresse à des populations (crypto, SSI, IR) aux parcours très différents.

- « Technique de recherche d'emploi »
  JP : bien mais trop tard dans l'année par rapport aux stages.
- « Anglais »
  JP : Groupes de niveau pas très bien faits. Pas assez de grammaire.
  CR : vous avez plus l'age de la grammaire, vous devez apprendre à vous lancer et à parler, peu importe les fautes de grammaire.
  En carte à puce on pourrait faire les présentations en anglais-> idée à garder pour l'an prochain.
- « CAP »
  JP : bien, les projets ont bien plu.
- « EEJE »
  JP : cours trop court
  SD : il y a eu un bug d'intervenant cette année et tous les cours n'ont pas pu être assurés,

Options

- « Protection de contenu »
  JP : intéressant
- « Protection de la vie privée »
  JP : cool, les TP ont plu, très bien pour la culture générale
- « Auth »
  JP :bien mais similaire à PVP
  PAF : ouverture d'esprit, TP bien séparés entre les 2 modules
  SD : je préviendrai l'an prochain.
- « programmation parallèle, GPU »
  JP : l'anglais ne pose pas de problème, un peu rapide sur la partie GPU
- « IDS »
  JP : très technique et éloigné de la crypto et trop dur
  PAF : c'est à ça que sert SRI : donner un aperçu sans rentrer dans les détails.

Point sur les stages

tout le monde a trouvé un stage cette année mais certains doivent être surveillés de près.

Bilan du premier semestre de M1

- « Algorithmique de base »
  MS : Très bien cours/TD. C'est bien qu'on passe tous au tableau en TD. Problème de synchronisation des TP avec les TP d'introduction à Sage d'ALGB. Un peu plus de détails sur les études de complexité.
- « Algèbre de base »
  MS : Partie Galois un peu brouillon au niveau du tableau. Difficile de se rattraper si on perd le fil. Que 3 TP un peu dommage.
- « Programmation scientifique 1 »
  MS : pas vraiment un cours. Travail à la maison avant le cours. Compliqué pour ceux qui n'ont jamais fait de C. trop axé modélisation et pas de crypto surtout pour le projet qui était trop orienté vers la physique. Parle trop de Fortran.
- « Probabilités pour la théorie de l'information»
  MS : plutôt bien. TD bien plu. Par contre le CC et l'examen sont trop éloignés des TD. Pas assez de temps sur la théorie de l'information. Pas de stats.

- ASR
  MS : trop rapide et presque rien sur architecture. TP java et ils connaissent pas le java. Tout en fin de semestre.
  SD : il y a eu un problème d'intervenant d'où la concentration en fin d'année.
- « Réussir son insertion professionnelle »
  MS : intervenant très bien mais ne connaît pas la crypto. Apprendre à écrire un CV et pas besoin de 6h pour ça.
  SD : c'est pas le but de connaître la crypto. Je préviendrai en début d'année.
- « Anglais »
  MS : personne n'ose parler. Idem M2, ils attendent de la grammaire
  SD : c'est à vous de vous lancer. Le but est de parler et de ne pas avoir honte de ses erreurs.
  Il faudrait multiplier les présentations en anglais dans la formation comme on le fait déjà en projet tutoré.

<u>Association des anciens étudiants</u>

Comme les années précédentes, l'association survit difficilement car personne ne veut y consacrer du temps. La page facebook semble à peu près vivante.