Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 29 janvier 2016

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

Bilan rapide des cours du second semestre de M1 2014-2015

« Crypto » OK, TD/TP vraiment bien pour compléter le cours
« Complexité » sympa mais pas assez de TD
« ACGA » très intéressant, cours difficile. Un peu trop rapide sur les aspects effectifs, éventuellement différentier les TD/TP/CC selon les populations
« COCO » super retours, génial
« Anglais » pas le plus apprécié
« projet tutorés » super retours, partie implémentation bien car ça permet de consolider ce qui a été fait en cours avant

Bilan des cours de M2

- **« Courbes algébriques »**
  Le cours est bien mais difficile, les TD/TP sont bien. Globalement, les étudiants sont un peu déçus par ce qu'ils ont pu faire à l'examen. L'an dernier il avait été demandé de faire un CC en milieu de module. Ça a été fait cette année et c'est positif.
- **« Théorie des nombres »**
  Module très intéressant, en particulier les TP (il y a beaucoup d'algos dans le cours). Ce serait bien de rajouter des TP mais pas au détriment des TD qui sont aussi très utiles pour comprendre le cours.
- **« Cryptographie avancée »**
  Très bien pour la partie asymétrique, sauf que les TP sont trop longs et qu'il faut découvrir magma. Ce serait bien de mettre en place une introduction un peu avant. Le choix de Magma semble bizarre pour le contest et comme c'est noté sur la progression les étudiants donnent leurs optimisations au fur et à mesure même si elles ont été trouvées au même moment. C'est dommage mais globalement la plupart des étudiants se sont pris au jeu et les résultats sont positifs.
  La partie symétrique est intéressante mais ça donne l'impression que ce n'est pas préparé, pas structuré et l'examen portait trop sur la fin du cours, déconnecté du cours.
- **« Programmation 1 (Java) »**
  Super cours, TP axés crypto, vraiment bien. Ça aurait été bien que ce soit pareil en C. Par contre ce n'est pas adapté aux étudiants de M1 qui n'ont pas encore fait de crypto à cette période de l'année.
  Il y a eu souvent des soucis avec ce cours qui s'est bonifié au fur et à mesure des années grâce au travail de ce comité.
  Il faudra cependant revenir à la situation précédente où ce cours n'était proposé qu'en M2.
- **« Cryptographie Quantique »**
  Bons retours, ce cours est apprécié mais il est très difficile et il n'y a pas assez de TD pour assimiler. C'est bien qu'il y ait un DM pour compenser.
- **« C++, les bases »**
  Bien car plein de TP et ce n'est pas grave si c'est du numérique. Une réflexion est nécessaire sur l'enseignement de la programmation : vaut il mieux approfondir un langage plutôt que saupoudrer plusieurs ? Cette question sera étudiée pour la prochaine habilitation, en particulier en regardant ce qui est fait ailleurs.
- **« Sécurité des Réseaux Informatiques »**

Très bien et intéressant mais il manque le bagage sur les réseaux heureusement qu'il y a les TP. Les intervenants sont bien mais ce serait bien d'avoir un document introductif pour chaque partie du cours. Cette question avait été soulevée l'an dernier et il semble quand même y avoir un mieux avec des petites introductions suivant les intervenants. Il faut donc persister. Le module ASR de l'an dernier avait été particulièrement mal fait ce qui explique aussi probablement ce manque de bagage.

- **« Technique de recherche d'emploi »**
  Très bons retours comme d'habitude avec en plus des entretiens blancs, des questions types et les réponses à y apporter. On va voir si on peut augmenter le volume horaire dans l'avenir en particulier pour des entretiens blancs.
- **« Anglais »**
  Comme d'habitude, ça ne sert pas à grand-chose. Les étudiants ne progressent pas. Malheureusement notre marge de manœuvre sur les enseignements d'anglais est très limitée.

Options

- **« Protection de la vie privée »**
  Le cours comme les TP sont vraiment très biens. Malheureusement, l'intervenant de ce cours (et de AUTH) part de Rennes.
- **« programmation parallèle, GPU »**
  Cours intéressant mais pas assez poussé sur les aspects GPU.
- **« IDS »**
  Cours plus structuré que SRI, TP bien.

Point sur les stages

C'est visiblement plus difficile cette année que les années précédentes en particulier pour les stages en entreprises. Actuellement seulement une grosse moitié des étudiants a trouvé un stage. C'est la même chose en SSI. Il faut vraiment encourager les étudiants à candidater sur Paris. C'est sûr que ce n'est pas idéal mais c'est là qu'il y a le plus d'opportunités (pour le stage et un premier emploi) et il ne faut pas le négliger.

Bilan du premier semestre de M1

D'une façon générale, l'origine des étudiants est très variée et les enseignants partent trop du principe que tout le monde a fait son cursus à Rennes. Il aurait également été mieux de prévenir plus tôt de la tenue de la réunion pour que la représentante puisse mieux s'organiser pour recueillir les avis de la promo (questionnaire anonymisé par exemple)

- **« Algorithmique de base »**
  Module très difficile, surtout sur la seconde partie. Très bien d'avoir un partiel au milieu. L'enseignant allait un peu vite sur les calculs de complexité et donnait les algorithmes optimisés (et donc plus difficilement compréhensibles) trop rapidement. Les étudiants ne connaissent pas tous sage (cf remarque préliminaire). L'équipe pédagogique va essayer de rédiger un TP d'introduction à sage que les étudiants devront faire en autonomie avant le premier TP de l'année.
- **« Algèbre de base »**
  Les étudiants sont mélangés avec les étudiants de maths fonda et les magistériens qui veulent aller plus vite. L'examen a porté sur la toute fin du cours ce qui explique la chute des résultats entre le CC et l'examen. Il n'y a pas de poly pour ce cours, mais par contre des références sont données sur la page du module. Encore une fois les étudiants n'ayant pas passé leur licence à Rennes n'ont pas nécessairement les prérequis à ce module (module ANAR de L3). Le responsable du cours s'adaptera l'an prochain (problème de langue et d'adaptation au public

cette année).
L'idée que ce module compte coefficient 6 au lieu de 9 dans la prochaine habilitation devrait être retenue pour donner moins d'importance à ce module.

- **« Programmation scientifique 1 »**
  Pas assez de crypto. C'est un module de C pour l'analyse numérique (pas motivant). L'enseignante fonctionne en cours inversé (uniquement des TP) et ça semble décontenancer les étudiants. Par contre au niveau du contenu, l'essentiel a été abordé. Le fait de faire le projet tutoré en C est une bonne chose pour pratiquer. Il devrait y avoir un module de C en SSI dans la prochaine habilitation, on a essayer de le mutualiser.
- **« Probabilités pour la théorie de l'information»**
  Gros décalage entre cours et TD. Il faudrait plus de TD sur la partie théorie de l'information et même imposer un moité/moitié en volume horaire dans ce module. Ce serait aussi bien d'y ajouter des bases de statistiques (jusqu'au chi 2 par exemple).
- **« Architecture, Système et Réseaux »**
  Il n'y a pas assez de cours et de TD ce qui en fait un module trop dense. Il manque une introduction car les étudiants partent pour la plupart de 0. Ce serait bien aussi d'avoir un lexique. Il est envisagé d'augmenter le volume horaire de ce cours dans la prochaine habilitation.
- **« Réussir son insertion professionnelle »**
  Les étudiants étaient réticents, mais l'intervenante était très bien et le contenu intéressant (entretiens, carrière, comment se présenter, pas trop de rédaction de CV)
- **« Anglais »**
  Trop hétérogène car pas de groupe de niveaux. Cours intéressant mais pas de progression des étudiants. Ça sert juste à maintenir son niveau d'anglais. Ça manque aussi d'ouverture dans les thématiques abordées.

<u>A modifier pour la prochaine habilitation (rentrée 2017)</u>

En général
Réfléchir à la place des enseignements de programmation (plusieurs modules du même langage pour approfondir pour un module de chaque langage pour en découvrir plusieurs). Regarder ce qui se fait ailleurs

M1S1

- Mettre ALGB coefficient 6
- Rajouter quelques TP en ALGB
- Augmenter le volume horaire de ASR
- Supprimer Java

M1 S2

- rajouter des TD en complexité
- rajouter des TD/TP en ACGA ou en faire des spécifiques (et du coup avoir une note finale différentes selon les populations)
- module de C à revoir ou faire en sorte qu'il y ait des TP de crypto. Tout en TP c'est pas si mal mais il faudrait un poly de cours très bien fait et des séances pour répondre aux questions (comme un vrai cours inversé)

M2 S1

- rajouter des TP en Théorie des nombres
- rajouter un ou 2 TP en Crypto avancée
- rajouter des TD en crypto quantique