Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 26 septembre 2019

Présents: Delphine Boucher, Mathieu Cima (M1 l'an dernier), Sylvain Duquesne, Elisa Lorenzo-Garcia.
Absents: Patrick Derbez, Eric Gousset, Pierre Loidreau, Blodwen Meynier (M2 l'an dernier), Christophe Ritzenthaler.

Bilan du second semestre de M1

- « Complexité»
  MC : très intéressant, CM comme TD appréciés par tous.
- « Codes correcteurs (COCO)»
  MC : très intéressant sans être trop simple et reste accessible à partir du moment où on s'y investit. Aide et écoute appréciés. Les challenges sont une très bonne idée, dommage que ce soit annoncé comme facultatif. C'est une très bonne alternative aux TP notés. Peut-être qu'un peu plus de retour serait bénéfique. Intéressant de se baser sur le NIST et en taille réelle → plus professionnalisant. Pas de soucis particulier sur la longueur des TP.
  DB: Les challenges, c'était une nouveauté, on va peaufiner cette année, voire les faire rentrer dans la note (là c'était juste en bonus).
- « Algèbre Commutative, Géométrie Algébrique (ACGA) »
  MC : trop volumineux et part du principe que les bases de la topologie algébrique sont acquises alors que ce n'est pas du tout le cas. Cours adapté au niveau ENS et du coup très difficile de ne pas perdre pied. Certaines remarques de l'enseignant ont été peu appréciées voire jugées désobligeantes (« il y a 2 publics dans ce cours, les mathématiciens et les autres », « les cryptos, c'est pas grave si vous comprenez pas »). Largués en TD et pas assez aidés. De même, les TP sont faits machinalement sans comprendre ce qui se passe. Attitude moqueuse voire méprisante des normaliens (cf ALGB au premier semestre), cette fois amplifiée par l'attitude de l'enseignant. Certains ne venaient plus en cours cause de çà. La partie GA n'était pas mieux en terme de contenu mais l'attitude de l'enseignant ne posait pas de problème.
  SD : Contenu du cours clairement mal adapté à la formation mais la partie sur les bases de Groebner devrait rester accessible et profitable.
  ELG/DB : Ce serait peut être bien de séparer les groupes ou de ne faire que la partie base de Groebner, éventuellement plus détaillée.
  SD : Il faut quand même trouver un cours pour compléter. Il n'y a malheureusement pas vraiment d'alternative économiquement viable. On va quand même essayer d'y réfléchir.
  Tous : Quelques soient les défauts de conception du programme du cours ou de la formation, les attitudes rapportées ne doivent pas se reproduire.
- « Cryptographie (CRYP)»
  MC : Rien à dire sur le cours. Ni trop simple, ni trop compliqué. OK en TD, niveau adapté à chacun. Petit bémol sur les Quizz car certaines questions étaient ambiguës mais l'enseignant a été réactif. Sujets de TP intéressants mais partaient du principe que python était maîtrisé ce qui n'était pas le cas. Là encore l'enseignant s'est adapté.
  ELG : Très difficile de faire un bon quizz car on ne peut pas s'appuyer sur la justification pour savoir si l'étudiant a compris.
- « Projet tutoré»
  MC : retours très différents. Intéressant, professionnalisant pour certains. D'autres ont souffert d'un mauvais « choix » de binôme. Certains auraient aimé être un peu plus guidés au moins au début car ils ne savent pas trop par où commencer et/ou n'osent pas demander de l'aide. Assez de temps pour travailler sur le projet.

  SD : C'est un problème récurrent. Les enseignants sont disponibles mais les étudiants ne viennent pas vers eux. L'aspect autonomie est fondamental pour se préparer aux stages et à l'insertion professionnelle. De même, apprendre à demander de l'aide est fondamental pour l'avenir professionnel.

MC : Pourquoi pas rendre facultative la mise en binôme ?
SD/ELG: Ca double la charge de travail pour les enseignants (rapports, soutenances) et surtout c'est important d'apprendre à travailler en équipe, même avec des personnes qui ne travaillent pas de façon satisfaisante (évidemment c'est mieux de ne pas tomber dans l'excès)

- « Anglais»
  MC : pas mieux qu'au premier semestre. De l'avis général le niveau est trop basique (raconter ses vacances, vocabulaire du cinéma) et pas assez professionnalisant (pas orienté maths et même pas sciences). En décalage avec le fait que certains cours du master sont en anglais.
  SD : C'est normal que les contenus ne soient pas crypto mais ils pourraient quand même être orientés sciences ou monde de l'entreprise pourrait. Ce sera remonté. Mais cette promo était particulièrement bonne en anglais. Le niveau doit rester accessible à tous les années à venir.
- Bilan global
  MC : Bon semestre à part ACGA. Appréciable de voir les outils du premier semestre appliqués à la crypto.
  SD : 14 étudiants étaient inscrits, 2 ont abandonné en cours d'année et les 12 autres ont validé l'année sans réelle difficulté, c'était une bonne promo.

Bilan du second semestre de M2
La représentante est absente mais a fait passer ses retours par email :
« Sécurité des implémentations (SIMP) » : Cours très apprécié, M.Gérard a été très pédagogue et a su montrer les différents points importants du cours. De plus les TP étaient ludiques et permettaient de bien comprendre les sujets vus en cours. C'est un des rares cours vraiment pratique.
« Courbes elliptiques pour la cryptographie (CEC) » : La suite logique de CBAL, pas de problème quant au contenu du cours, ni à celui des TD. Les étudiants ont été assez surpris par le contrôle continu qui demandait une rapidité à laquelle ils ne s'étaient pas exercés. A la fin, le cours et le TD se sont un peu éloignés l'un de l'autre.
« Théorie algorithmique des nombres (TANC) » : C'est un peu dommage de l'avoir vu comme un catalogue d'algorithmes et surtout l'examen ne correspondait pas à ce qui avait été fait en cours dans la forme
« Stages » : finalement, dans le privé, rien ne se débloque avant fin octobre, pas la peine de paniquer avant. Il aurait été apprécié d'avoir un suivi un peu plus personnalisé que la semaine profil pour la préparation aux entretiens et la construction d'une lettre de motivation. Mais ce n'est vraiment pas primordial.

Le point le plus important était une mauvaise organisation de la session 2 (quels modules ont une session 2, quels étudiants sont concernés ?).
SD : On a essayé de rattraper au mieux. Cette année il n'y a plus de session de rattrapage en M1 et peu en M2 (MCC disponibles sur l'ENT). Il y a toutefois possibilité d'épreuves de substitution pour les absences justifiées.

Bilan des stages de M2
SD : Encore une fois, les stages se sont globalement très bien passés. Il y avait 15 étudiants présents. 2 n'ont pas validé l'année et redoublent. A ce jour 9 des 13 étudiants qui ont validé leur année ont trouvé un emploi ou une thèse et 2 ont choisi de se réorienter. Il y avait 4 étudiants en Allemagne et 3 ont validé l'année (c'est classique que les étudiants du double diplôme mettent un peu plus de temps car le stage commence plus tard).

Point sur la rentrée
72 candidatures ont été reçues en M1 dont 20 de l'étranger. C'est moins que l'an dernier au global mais la baisse vient uniquement de Campus France qui opère une présélection de plus en plus drastique. Cela n'empêche pas que les candidats acceptés ont des difficultés pour venir (finances, visas).
38 ont été acceptés (+7 sur Campus France) et finalement seulement 14 inscrits (+1 Campus France mais qui n'a toujours pas obtenu son visa). C'est du à des désistements de dernière minute (étudiants

administrativement inscrits qui ne sont finalement pas venus). La question se pose de savoir si il faut en accepter plus ou avoir des plus petites promos mais d'un meilleur niveau. L'avis global est que c'est mieux de ne pas avoir une trop grosse promo.

En M2, il y avait 18 candidatures qui n'avaient pas fait le M1 crypto à Rennes. 5 ont été acceptées et 3 sont venus. La plupart viennent dans le parcours recherche car les prérequis sont importants pour le parcours classique et donc difficiles à rattraper.
Il y a finalement 17 étudiants inscrits dont 4 dans le parcours recherche. Il faut rajouter à cela 2 étudiants du double diplôme actuellement en Allemagne. Il y a également 2 étudiants du M2 mathématiques fondamentales qui suivent le cours de courbes elliptiques.

MC : Craintes sur l'emploi du temps à cause de ce qui s'est passé l'an dernier et inquiétude des étudiants du parcours recherche qui ont peu de cours en ce début d'année et craignent une surcharge pour la suite
SD : L'emploi du temps est mieux réparti cette année grâce aux aménagements effectués suite aux problèmes de l'an dernier. Le cours de Réseaux euclidiens a dû être déplacé au second semestre pour des raisons de disponibilité des intervenants ce qui explique en partie l'impression des étudiants du parcours recherche. On va essayer de faire commencer le cours de codes correcteurs en fin de S1 pour équilibrer.
Reste quelques bugs avec le séminaire, C++, CS et SEP. Malheureusement, on ne peut rien y faire car ces cours dépendent d'autres formations.
Les étudiants de M1 s'interrogent également sur l'utilité de l'histoire des maths. C'est un cours de culture mathématique, ce qui a un intérêt en soi pour tout étudiant de mathématiques. Certains étudiants l'apprécient d'ailleurs. C'est vrai que ça pourrait être une option (mais personne ne le choisirait) et dans tous les cas il ne compte pas pour beaucoup (1/6 de la note de projet tutoré).