Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 8 février 2018

Présents: Delphine Boucher, Sylvain Duquesne, Eric Gousset, Pierre Loidreau, Elisa Lorenzo Garcia, Blowden Meynier (M1), Sarah Paardekooper (M2), Andy Russon (M2)

Excusés : Christophe Ritzenthaler

Absents : Patrick Derbez

Composition du comité

Andy Russon remplace Sarah Paardekooper comme représentant des M2 dans le comité. Eric Gousset (également membre du conseil d'UFR) remplace Kelly Resche comme représentant d'Amossys dans le comité.

Bilan du premier semestre de M1

Les notes n'ont pas été communiquées aux étudiants alors que le jury a eu lieu. En fait, le master est maintenant cohabilité avec Brest par exemple ce qui fait que le jury officiel a lieu plus tard (une fois que tous les jury de site se sont réunis). Avec les précautions d'usage, les notes peuvent être communiquées directement par les enseignants.
Pas de choix d'option en M1, à la fois pour des raisons budgétaires, d'emploi du temps et de cohérence du parcours (bases communes sur lesquelles on peut s'appuyer en M2)

- **« Algorithmique de base »**
  BM : Pas assez de démonstration et du coup c'est difficile de savoir ce qui est attendu. Trop d'apprentissage des algorithmes sans connaître les raisons, le cadre, les objectifs et quelles sont les compétences attendues en fin de module. Les étudiants ont eu du mal à trouver le fil conducteur du cours, les liens entre algorithmes et théorèmes. Peu de lien entre les 2 parties.
  EL/DB : Bien sûr, il ne faut pas apprendre les algorithmes par cœur mais il faut les comprendre.

  Il faudrait revoir les MCC en passant tout en CC car actuellement il y a un déséquilibre du à la règle du max et c'est plus adapté à ce module.
  Il faut mettre plus en avant les objectifs du module et l'afficher plus clairement. En particulier le fait qu'il n'y ait pas de lien entre les 2 parties doit être annoncé. Mais c'est vrai que c'est un module avec une dimension un peu culturelle et sur certains sujets, ca reste superficielle et c'est probablement ca qui donne cette impression de patchwork. Pourquoi pas donner une coloration un peu crypto/codes au moins dans les motivations.

- **« Algèbre de base »**
  BM : Plutôt bon avis de la part d'une bonne partie des étudiants mais retours plus sévères de la part des autres. Le cours va très vite mais ça se comprend et il est plutôt bien. Par contre, il manque d'exemples et c'est reproché par l'enseignant de théorie des nombres en S2. L'enseignant de TD fait indépendamment de si les étudiants comprennent ou pas, ne se met pas assez au niveau des étudiants alors qu'il y a un groupe de TD spécifique crypto exprès pour cela. Une note de passage au tableau en TD a été introduite et semble inégalitaire. Ca aurait un sens si c'était un bonus mais là ca enfonce les étudiants en difficulté.
  Le cours est trop dépendant des modules de L3 de Rennes alors que ce n'est pas le cas de la majorité des étudiants voire certains n'ont pas fait d'algèbre générale en L3.
  Pourquoi ne pas faire un examen différent selon les populations ?

SD : C'est un module habituellement difficile (et d'ailleurs le coefficient a été baissé dans le calcul de la moyenne semestrielle par rapport au nombre de crédits ECTS qu'il vaut). L'enseignant de TD sera briefé l'an prochain. Un examen séparé est administrativement impossible mais on peut réfléchir à la création d'un cours spécifique (mais sans enseignement spécifique). En ce qui concerne la note de passage en TD, il semble qu'il n'en ait pas été tenu compte dans le calcul de la note de CC finale, en tous cas pour les étudiants qui ne sont pas passés au tableau.

- **« Programmation scientifique 1 »**
  BM : Très mis à l'écart par rapport aux CSM mais le cours est agréable. Projet sans communication entre les élèves et sans choix du binôme (en fonction du niveau supposé) → ça a perturbé les étudiants. Polycopié et cours très bien fait même pour ceux qui n'ont jamais fait de C ou ceux qui en ont déjà fait. Pas forcément idéal quand les étudiants ne font pas exactement la fonction attendue et du coup pas d'explication sur pourquoi les programmes ne fonctionnent pas.
  SD/PL : C'est du C pour numériciens mais avec des TP spécifiques. Attention, ce n'est pas facile (et ca prend beaucoup de temps) pour un enseignant de comprendre d'où vient l'erreur d'un programme original.

- **« Probabilités pour la théorie de l'information»**
  BM : TB mais très minime sur la théorie de l'information. Surtout que les étudiants sont frustrés par rapport à la quantité d'algèbre. Polycopié très bien fait.
  SD : C'est normal qu'il y ait peu de modules appliqués au premier semestre. Ca évoluera au second, mais ça reste un master de maths avec une partie mutualisée avec les parcours maths fondamentales (et donc plus théorique).

- **« Architecture, Système et Réseaux »**
  BM : Très utile surtout qu'on y connaît rien au début. Pas assez de TP. Pourquoi pas avec du travail à la maison. Quitte à enlever un peu de cours surtout la fin qui semblait moins fondamentale. Par contre les TD sont bien.
  EG : pourquoi c'est si utile.
  BM/SD : ca permet de connaître le contexte dans lequel on fait de la crypto et d'être ouverts.
  EG : C'est très bien et très important effectivement.
  SD : On va voir avec l'enseignant pour rajouter quelques séances de TP en échange de quelques séances de cours.

- **« Anglais »**
  BM : Projet de 2eme partie de semestre très bien mais presque trop libre. Pas assez encadré, en particulier sur le timing. Le but c'est juste de continuer à pratiquer en dehors des cours et en particulier en fin de semestre.

- **« Semaine Profil »**
  BM : Inscriptions galères et les étudiants passent à coté de bons ateliers. Par contre les ateliers et les conférences sont très bien. Trop de sophrologie, pas assez d'entretien (en anglais, un seul groupe). Très intéressante.
  SD : ces retours seront remontés au SOIE pour qu'il en soit tenu compte l'an prochain.

<u>Bilan du premier semestre de M2</u>
SP : Déséquilibre du semestre au niveau difficulté et au niveau emploi du temps. Pas assez de cours en décembre et surtout en Janvier/Février. Très lourd en Oct/nov surtout avec les rapports à rendre et les stages à chercher.
SD : Le cours de courbes elliptiques a été déplacé cette année au second semestre à la place d'ALCO

(transition entre les maquettes). On pourrait pérenniser ce report (même si il compte pour le premier semestre pour alléger un peu le premier semestre)

- **« Courbes algébriques »**
  SP : Pas assez de démonstrations. C'est vrai que c'est du théorique mais ça permet de mieux comprendre. Ce serait bien d'avoir un polycopié ou un livre pour s'appuyer dessus dès le début du cours. Ca permet de poser des questions sans avoir peur d'être en retard et de pouvoir se raccrocher après. Examen plus dur que l'an dernier. C'est dur, mais c'est une bonne chose de le faire en anglais.
  EL : livre non donné en début de cours de peur que les étudiants ne suivent pas voire ne viennent pas, mais si c'est mieux au début, ce sera fait comme ça l'an prochain. Les résultats sont meilleurs que l'an dernier.
  EG : l'anglais est indispensable. C'est éliminatoire dans les écoles d'ingénieur et de plus en plus demandé dans les offres d'emploi. Autant un employeur peut difficilement exiger la maîtrise d'une compétence technique spécialisée, autant l'anglais est la base de toute communication actuellement et ne peut pas s'acquérir en quelques semaines si besoin.
  SD : c'était imposé dans les nouvelles habilitation d'avoir au moins un cours en anglais par an. Par contre si il y a un examen, il doit être en français.

- **« Réseaux euclidiens en cryptographie »**
  SP : Cours et profs intéressants. Un peu difficile. Ça mériterait plus de 3 ECTS car il y a pas mal d'heures de cours.
  SD : Le nombre d'ECTS n'est pas vraiment important. On ne peut pas changer car c'est un module partagé avec le master cybersécurité (c'est d'ailleurs pour ça qu'il y a plus d'heures de cours). Par contre, le coefficient pour le calcul de la moyenne sera augmenté en fonction du volume horaire pour l'an prochain.

- **« Cryptographie quantique »**
  SP : Presque pas de TD. Dommage car c'est très intéressant. TB d'avoir le cours en pdf. Examen pas très représentatif du niveau. Ça pourrait être un DM. L'évaluation est trop « facile » par rapport au cours.

- **« Programmation 1 (Java) »**
  SP : Peu intéressant. Premier TP très compliqué. 2 fois plus d'ECTS que les autres matières. Python serait plus intéressant. Les étudiants pourraient l'apprendre par nous même sauf les TP.
  SD : Java est très important en entreprise. Python est plus intéressant pour la crypto mais pas pour le développement logiciel en entreprise et surtout le. C'est un cours de Licence info mutualisé ce qui explique qu'on n'attend pas la même maturité et autonomie que celle d'étudiant en M2. Il faut bien distinguer C et Java (le but est d'apprendre à maîtriser un langage de programmation) et Sage/magma qui servent d'outils d'illustration et d'application pour les cours. En ce qui concerne les ECTS, là encore le coefficient sera diminué l'an prochain.
  EG/PL : Le python est de plus en plus utilisé mais cache plus les structures de données (c'est un langage pratique). Java reste la référence.

- **« Sécurité des Réseaux Informatiques »**
  SP : Avis partagés. Cours donnés par des professionnels mais trop d'intervenants différents sans liens entre eux. C'est très bien mais les TP sont désynchronisés du cours. Pas assez de place en salle de TP et de loin !
  SD : des salles de TP spécifiques aux formations en sécurité devraient être crées.

- **« C++, les bases »**
  SP/AR : intéressant. Très complet. Enseignant disponible et très compétent. Par rapport au

java, ils apprennent plus de choses qu'ils ne pourraient pas apprendre tout seul. Ce serait bien d'avoir accès à la suite.
SD : La deuxième partie du module n'a aucun interet car très axée sur le calcul numérique.

- **« GPU »**
  SP/AR : Cours très intéressant. Pas assez de TP sur la partie GPU. Cours en anglais mais pas d'un niveau terrible (pour la deuxième partie).

- **« Sécurité des données pour la propriété intellectuelle et la vie privée »**
  SP : Problème au début mais cours très intéressant.
  SD : Il y a eu un gros problème au début de l'année car Supelec (propriétaire du module) n'était pas au courant que les étudiants de crypto y participaient au module. Ils ont finalement accepté que les étudiants y assistent et l'évaluation a été faite sur une étude de texte par SD et Caroline Fontaine (intervenante dans le cours). Cette question sera bien sur réglée pour l'an prochain.

- **« Sécurité des systèmes d'exploitation »**
  SP : Niveau très élevé sans être prévenus en avance. Prérequis importants. Évaluation sur articles mais pas tous du même niveau (un fait 150 pages). Mauvaise organisation des oraux.
  SD : Ce module est nouveau et nous n'avions donc pour l'instant pas de retour. Les prochaines promos seront informées.

- « **Résolution de challenges de sécurité** »
  SP : Plusieurs intervenants. Les étudiants ne savent pas comment ils sont évalués. Manque d'organisation. Aucune information sur l'évaluation.

- **« Protocoles de sécurité »**
  SP : Positif, projet bien et motivant. Notions assez faciles (en tous cas du point de vue intuitif, le formalisme est plus difficile) et du coup on pourrait passer moins de temps en cours et plus en TP.

- **« Géométrie et arithmétique des courbes algébriques»**
  SP/AR : Très difficile mais très intéressant. Et pas assez de temps libre dans l'emploi du temps pour travailler sur ce cours comparé au M2 maths fondamentales.

- **« Anglais »**
  SP : Manque d'organisation des oraux (pas assez d'explication par oral). Beaucoup de travail en dehors des cours.

- **« Semaine Profil »**
  AR : inscription pas du tout ergonomique. Il faut cliquer partout. Ateliers intéressants pris d'assaut. Et il reste malheureusement quelques cours pendant cette semaine là.

<u>Point sur les stages</u>
3 étudiants (étrangers, probablement défavorisés par la thématique) sur 17 n'ont pas encore trouvé de stage à ce jour. 9 vont en entreprise et 4 en labos.

Amossys aimerait un retour sur l'intervention pour l'améliorer. AR donne son avis personnel (intéressant) mais ce point sera réévoqué au second semestre.