Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 31 janvier 2019

Présents: Delphine Boucher, Mathieu Cima (M1), Sylvain Duquesne, Pierre Loidreau, Blowden Meynier (M2)

Excusés : Christophe Ritzenthaler, Elisa Lorenzo Garcia,

Absents : Patrick Derbez, Eric Gousset

Bilan du premier semestre de M1

Les notes n'ont pas été communiquées aux étudiants alors que le jury a eu lieu. Le master est cohabilité avec Brest ce qui fait que le jury officiel a lieu plus tard (une fois que tous les jury de site se sont réunis). Finalement le jury officiel aura lieu en fin d'année et les notes ont été communiquées aux étudiants.

MC : Au niveau global sur le semestre, c'était chargé en terme de volume horaire. Cours très intéressants mais pas forcément en lien avec la crypto. Ce serait pas mal d'accentuer un peu sur les cours spécifiques à la formation.

SD : C'est normal qu'il y ait peu de modules appliqués au premier semestre. Ça évoluera au second, mais ça reste un master de maths avec une base mutualisée avec les parcours maths fondamentales (et donc plus théorique).

- **« Algorithmique de base »**

  MC : Rien à redire sur la première partie. Pas évident d'identifier ce qui était le plus important dans le cours. Manque une introduction à Sage. Certains étudiants se retrouvent donc en difficulté. Examens un peu trop longs.

  Pour la seconde partie, Pas de soucis en cours mais ce serait bien d'avoir des corrections complètes de TD et d'être un peu plus guidés pendant les TP.

  DB/SD : Il devrait y avoir des TP de Sage en ALGB qui servent d'introduction. Ils n'ont pas été faits. Cela va être remonté à l'UFR Maths.

  BM : L'an dernier la plupart des étudiants de maths fondas ne venaient pas en TP.

- **« Algèbre de base »**

  MC : Cours très bien fait, en particulier les tests de primalité. Très clair. Le gros bémol c'est que le cours est partagé avec les normaliens. Au delà des écarts de niveau, ça se ressent dans l'ambiance et certains craignent de poser des questions de peur de la réaction des normaliens. Des réactions hautaines voire méprisantes ont été relevées (« vous faites pas des vraies maths », « c'est quoi cette question trop évidente », « trop trivial ») y compris envers le professeur. TD très bien, mais une correction finale plus rigoureuse serait appréciable car il n'est pas évident de manier correctement les différents outils mathématiques. Bien adapté au niveau général, c'est très bien qu'il y ait un groupe spécifique crypto.

  DB/SD/PL : Le groupe spécifique crypto semble porter ses fruits par contre cette mentalité des normaliens en cours est inquiétante et inacceptable. Ce sera remonté à l'ENS. On peut comprendre des soucis de différence de niveau mais on avait jamais eu de tels retours.

  BM : l'an dernier les normaliens venaient peu en cours

- **« Programmation scientifique 1 »**

  MC : très intéressant et très utile. On apprend vraiment à programmer. Certaines parties du cours traînent un peu en longueur (environnement unix) et d'autres mériteraient d'être un peu approfondies (utilisation des pointeurs). Pas de problème particulier de mélange avec les étudiants de CSM. Petit soucis pédagogique sur le discours du prof quand il dit que c'est facile et qu'il n'y a pas besoin de réfléchir alors que ça ne l'est pas pour tout le monde. Surpris de

passer à Python en S2 (Crypto).
SD/DB : C'est une très bonne chose que ce cours soit enfin bien adapté à la formation. Le C ressert en projet tutoré et il est important d'apprendre à manipuler un nouveau langage car c'est une situation très courante dans le monde professionnel. Le chargé de TP mettra en place une introduction à Python par rapport à Sage dans l'avenir.

- **« Probabilités pour la théorie de l'information»**
  MC : Rien à redire, très bien fait et très apprécié en particulier la théorie des codes. Parfois un peu trop d'aspects fondamentaux sur la théorie des probabilités.

- **« Architecture, Système et Réseaux »**
  MC : TD et TP très bien et très instructifs. Correction TB. On apprends moins en CM, ca vaudrait peut être plus le coup de faire moins de CM et plus de TD/TP. Pas toujours très clair sur ce qui est attendu en examen. Pas de problème de prérequis.

- **« Anglais »**
  MC : Regroupement avec les CSM à cause du faible effectif (et du coup changement d'intervenant pas forcément heureux par rapport à l'an dernier...). Pas le cours le plus enthousiasmant. Pas en lien avec les maths et les sciences. Trop académique.
  SD : C'est normal que ce ne soit pas en lien avec les sciences. L'objectif c'est de savoir communiquer (pour un entretien par exemple). La science ça vient tout seul ensuite et c'est pas le plus difficile.
  MC : Peut être plus l'orienter vers le monde professionnel.

- **« Histoire des maths »**
  MC : Plutôt une bonne surprise. Très bonne idée d'avoir intégré cette UE. Prof très compétent mais le programme était un peu trop chargé état donné le volume horaire. Pas clair comment serait faite l'évaluation. Manque un peu de vivant, de concret. C'était annoncé et voulu mais au moins en introduction, ça permettrait de motiver un peu plus.

- **« Semaine Profil »**
  MC : Pas trop de soucis pour s'inscrire. Le forum était bien. Les conférences très inégales. Ateliers pas terribles alors que les sujets étaient alléchants, en particulier à cause des intervenants pas forcément les plus compétents ou enthousiasmants voire impliqués.
  BM : Moins de conférences intéressantes que l'an dernier car pas adaptées à la formation. Peu de stands intéressants par rapport à la formation au forum et rapidement recalés (veulent des informaticiens). Même impression que les M1 sur les ateliers (assez vendeurs à priori mais pas grandioses au final).
  BM/MC : Très bien que l'emploi du temps ait pu être adapté

  SD : L'information de s'inscrire vite a permis d'avoir les ateliers/conférences demandées, mais ca fait bien maigre comme retour positif… Pour le forum, ça doit être spécifique aux entreprises présentes cette année (ou à leurs représentants qui ne maîtrisent pas forcément tous les besoins de l'entreprise) car globalement la demande crypto est toujours forte. Ces retours seront remontés au SOIE pour qu'il en soit tenu compte l'an prochain.

<u>Bilan du premier semestre de M2</u>

SD : l'emploi du temps était catastrophique ce semestre. Aucune spécificité par rapport à l'an dernier ne l'explique. C'est essentiellement dû à une accumulation de modules optionnels en octobre/novembre issus d'autres formations et sur lesquels on a donc aucun contrôle. Des mesures seront prises l'an prochain pour éviter que cela se reproduise comme déplacer officiellement certains

cours au second semestre, supprimer l'option SSE, mieux répartir dans l'année.
BM : Certaines semaines vraiment très chargées avec tous les créneaux pris toute la semaine alors qu'en ce moment il y a très peu de cours. Seul Challenge de sécurité a débordé en janvier. SIMP pourrait aussi être décalé entièrement en janvier/février.

- **« Courbes algébriques »**
  BM : Assez flou. Pas clair ce qui est important ou culturel. Par exemple, des choses vues très rapidement en cours se retrouvent à l'examen et inversement. Difficile de faire le lien entre le cours, l'examen, les TD. Difficile de mémoriser des théorèmes sans savoir à quoi ils servent (couplage de Weil par exemple). TP pas forcément utiles sur le coup et pas d'implémentation (juste de la découverte de ce qui existe dans sage). Ils n'apportent pas grand-chose. Çà s'éclaire un peu plus avec le cours de courbes elliptiques pour la cryptographie ou en théorie algorithmique des nombres.
  Difficile à suivre le cours en anglais pour certains mais globalement, même si ca demande plus de concentration, ça se fait et c'est ressenti positivement.
  DB : C'est bien qu'un cours soit en anglais
  SD : Le contenu va être revu avec la responsable du cours

- **« Réseaux euclidiens en cryptographie »**
  BM : Mitigé sur la difficulté. Certains ont trouvé la première partie trop difficile, d'autres la seconde. On sent pourtant beaucoup d'efforts pour faire comprendre les choses. TD de la première partie TB et ceux de la seconde très difficiles. Il faut dire aussi que ce cours est tombé en plein dans la partie la plus chargée de l'emploi du temps. Pas facile de s'accrocher sur la première partie car peu de traces écrites.
  Sur la seconde c'est plus le fond qui est dur car poly très bien fait et apprécié. Récapitulatifs également très appréciés.
  SD/PL : C'est apparemment la partie preuve de réduction qui pose problème car c'est des choses difficiles. On va voir avec les intervenants si on peut l'alléger d'autant que ce n'est pas spécifique aux réseaux. On va aussi voir si on peut fournir des références ou un support pour la première partie du cours.

- **« Cryptographie quantique »**
  BM : Module très resserré sur l'emploi du temps et donc difficile de tout assimiler. Manque un peu d'exemple mais enseignant très pédagogue, TD très bien faits, ce qui est attendu est clair.
  SD/DB : ce cours est indépendant du reste de la formation et pourrait donc être mieux placé dans l'emploi du temps.

- **« Programmation 1 (Java) »**
  BM : TP très ciblés crypto et donc très intéressants mais très lourds et très longs à faire d'une semaine sur l'autre. Consignes parfois manquantes. Trop peu d'explications sur les notes. Difficile de progresser. TP1 assez raide alors que les suivants (le dernier sur RSA par exemple) sont plus faciles. Pas de lien entre les TD (qui n'avancent pas, dans un environnement très bruyant) et les TP. Les feuilles de TD sont intéressantes mais la plupart des choses ont déjà été faites au préalable en TP. Étonnant que ce soit le module qui compte le plus alors qu'il n'est pas central en crypto.
  SD/DB : savoir programmer objet c'est plus qu'utile, c'est indispensable. Le nombre de crédits ECTS est essentiellement dépendant du volume horaire qui est important pour ce module. On peut éventuellement jouer sur le poids dans le calcul de la moyenne mais les notes ne sont pas spécialement mauvaises. On va quand même voir avec l'enseignant pour étaler un peu plus le rendu des TP et mieux articuler TD/TP.
  BM : Pourquoi pas plutôt le C++, par exemple utilisé en SIMP
  SD/PL : Les TP orientés crypto sont intéressants et on ne les aura pas en C++. Mais il faut

effectivement plus communiquer sur l'importance de C++ à la réunion de rentrée. Entre Java et C++, ça dépend de ce qu'on fait : en R&D c'est plutôt du C++ mais en applicatif, c'est plutôt du java car très portable.

- **« Sécurité des Réseaux Informatiques »**
  BM : Cours très intéressants mais TP peu basés dessus. Manque les bases, de recul pour profiter des TP vraiment difficiles d'autant qu'on est mélangés avec des master réseaux. Beaucoup de bonne volonté du prof (mais il répond peu aux emails).
  PL : Même retour tous les ans.
  SD : Pas nouveau effectivement mais important d'avoir les bases de la sécurité réseau. Ça a déjà été discuté avec l'intervenant d'avoir des documents sur lesquels s'appuyer.
  BM : Pourquoi pas mettre des sujets de TP un peu plus light ou des questions plus détaillées.

- **« C++, les bases »**
  BM : Super, très clair. Un cours un peu plus avancé serait pas mal, surtout en TP.

- **« GPU »**
  BM : TB. Pas de soucis avec l'anglais. Consignes parfois un peu vagues en TP. Interrogations sur la présence et les interventions de Mme Dunseath-Terao pendant les cours.

- **« Sécurité des données pour la propriété intellectuelle et la vie privée »**
  BM : 4h de cours d'affilé c'est fatiguant. Aucun TD, du coup on sait pas trop à quoi s'attendre.
  SD : C'est classique des cours de M2 qu'il n'y ait pas de TD, c'est un module avec le parcours recherche en informatique

- « **Résolution de challenges de sécurité** »
  BM : TB mais ne savent pas comment ce sera noté. N'apporte pas forcément grand-chose par rapport à la formation.

- **« Protocoles de sécurité »**
  BM : très formel, pas de séance de TD pour pouvoir comprendre. Il y a des feuilles d'exo quand même mais sans méthode ni correction. Par contre le projet était TB mais pendant la période trop chargée et tout le monde n'a donc pas pu y mettre l'investissement nécessaire.

- **« Cours du Master recherche»**
  BM : Très chargé et examen difficile

- **« Anglais »**
  BM : Bien. Nécessaire et permet de changer d'air.

- **« 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>
SD : 2 étudiants sur 16 n'ont pas encore trouvé de stage à ce jour.
BM : On y peut rien mais la recherche de stage est éprouvante et génératrice de stress et d'absence pile pendant la période surchargée. Difficultés pour savoir où postuler. Heureusement qu'il y a les offres envoyées sur la liste et la liste d'entreprises distribuée en début d'année.
BM : D'un point de vue général, ça aurait été bien que les profs soient informés de la surcharge ce qui aurait évité des remarques désagréables du type « il faut vous mettre à bosser ».
Pourquoi ne pas faire la cryptanalyse de l'AES en M1. Ça aurait permis de mieux comprendre l'AES

pour l'implémenter en M1, d'être réutilisé en SIMP et ça n'a de toutes façons rien à voir avec la théorie algorithmique des nombres
SD : Trop tard pour cette année, mais c'est une suggestion à creuser

Opportunité de cours de codes correcteurs pour la cryptographie

Ce serait bien d'avoir un tel cours au vu de l'évolution actuelle. Mais il faut le faire à budget constant, c'est à dire à la place d'un autre cours. Il ressort de la discussion engagée par le comité.

- Les cours de Courbes algébriques et courbes elliptiques pour la cryptographie sont regroupés et on en enlève les parties les moins importantes (géométrie projective par exemple, difficile à comprendre et pas vraiment utilisée dans la suite). Ce cours ferait 5 ECTS et 44h. **SD** et **ELG** vont discuter du contenu. Si besoin en sollicitant l'UFR pour quelques heures de plus (mais de toutes façons pas trop vu la surcharge constatée cette année).
- Un cours de cryptographie basée sur les codes de 2 ECTS et 18h est crée au second semestre.
- Cryptographie quantique passe au second semestre (ce qui permet d'alléger le premier).
- **PL, DB** et Julien Lavauzelle réfléchissent au contenu, à l'articulation avec le cours de M1 et à la répartition horaire CM/TD/TP ou projets et seraient susceptibles d'assurer ce cours. Gwezenheg Robert et Benoît Gérard pourraient également intervenir.