Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 25 septembre 2020

Présents: Romane Arvier (en visio, M1 l'an dernier), Delphine Boucher, Sylvain Duquesne, Pierre Loidreau, Elisa Lorenzo-Garcia (en visio).
Absents: Mathieu Cima (M2 l'an dernier), Patrick Derbez, Christophe Ritzenthaler.

Bilan du second semestre de M1

RA : Globalement compliqué avec le confinement. A part COCO et CRYP, tout n'a pas été fait. Sinon le début du semestre ca allait et ca reste un bon semestre. Pas trop de difficultés techniques pour pouvoir suivre les cours en ligne

SD : COCO et CRYP sont les cours les plus importants du semestre. C'est donc un moindre mal et il ne devrait pas y avoir trop de séquelles en M2.

- « Complexité»
  RA : Les classes de complexité n'ont pas pu être abordées.
- « Codes correcteurs (COCO)»
  RA : TB
  DB : Ca va être très compliqué cette année car il y aura 50 étudiants en comptant ceux de maths fondamentales.
- « Algèbre Commutative, Géométrie Algébrique (ACGA) »
  RA : très dur, surtout pendant le confinement (seulement des poly, pas de cours et donc pas d'explication)
  SD : Ce cours a été remplacé par Machine learning cette année
- « Cryptographie (CRYP)»
  RA : manque de cohérence entre les TP (sage) et l'AES (C) qui a déstabilisé. Les étudiants avaient l'impression d'avoir réussi et ont été surpris du message de l'enseignant exprimant l'impression inverse.
  SD : le message s'adressait maladroitement à toute la promo alors que les résultats étaient hétérogènes.
- « Anglais»
  RA : changement positif par rapport au premier semestre et aux retours de l'an dernier. Contenu basé sur la préparation de CV, lettre de motivation et d'entretiens → très motivant.
- « Projet tutoré»
  SD : les soutenances n'ont pas pu se dérouler. Comment s'est déroulé le travail, en particulier à distance pour un travail en binôme.
  RA : les étudiants qui ont sollicité les enseignants par mail ont eu des réponses rapides. Le travail en binôme est compliqué à distance mais la fin a pu se faire hors confinement pour plusieurs d'entre eux

SD : 16 étudiants étaient inscrits, 3 ont abandonné en début d'année et les 13 autres ont validé l'année sans réelle difficulté, c'était une bonne promo.

Bilan du second semestre de M2

Le représentant est absent mais a fait passer ses retours par email :
« Réseaux euclidiens en cryptographie (REC) » : une partie des cours n'a pas eu lieu en raison des mouvements sociaux. Cours très intéressant et bien adapté aux objectifs du master. Très bien structuré, complexité graduelle, les polycopiés de CM résumaient parfaitement le plus important de chaque partie. TD cohérents avec les CM. L'examen a paru compliqué pour la grande majorité des étudiants sans être impossible non plus.
« Théorie algorithmique des nombres (TANC) » : Les cours n'ont pas eu lieu en raison des mouvements sociaux
« Cryptographie quantique (CQ) »: Très intéressant, mais exercices très complexes. Beaucoup ont vite décroché, malgré une volonté de vouloir continuer beaucoup aidé par un professeur très impliqué et toujours prêt à aider ses étudiants. Examen trop dépendant des documents (autorisés) à disposition → écart-type important (plus de 7).

« Anglais » : Même constat qu'en M1 : les cours ne sont pas adaptés à la vie professionnelle. Il serait vraiment appréciable d'orienter le cours vers certaines bases du monde d'entreprise tel que les formulations d'un mail pro en anglais ou du vocabulaire propre à l'entreprise en anglais. Pour les aspects techniques, les cours en anglais comme GPU ou courbe elliptique 1 sont une très bonne chose.

Bilan des stages de M2

Retour des étudiants : Obtention des stages très variable. Certains avaient déjà un stage début novembre et d'autres cherchaient encore en janvier. De façon générale, trouver un stage n'a pas été compliqué.
Expériences variables aussi durant le stage. En général très positif, jusqu'à une offre d'emploi, mais quelques mauvaises expériences.
Ceux qui cherchent encore un emploi ne se font pas de soucis sur l'issue malgré la situation actuelle au vu des entretiens qu'ils ont passés depuis la fin de leurs stages.

Le confinement a aussi été vécu/géré très différemment en fonction de l'entreprise et/ou du pays

SD : Encore une fois, les stages se sont globalement très bien passés. Il y avait 15 étudiants présents qui ont tous validé l'année. A ce jour 10 d'entre eux ont trouvé un emploi. La plupart de ceux qui n'ont pas trouvé n'avait pas ou peu cherché avant la fin de leur stage. Il semble que la situation sanitaire n'ait pas vraiment eu d'impact sur les débouchés car ces chiffres sont similaires aux années antérieures ou une thèse. Il y avait 2 étudiants en Allemagne dont un a validé l'année (c'est classique que les étudiants du double diplôme mettent un peu plus de temps car le stage commence plus tard). A noter tout de même que cette année est la dernière pour le double diplôme. L'expérience a été très positive pour les étudiants concernées mais cette possibilité n'intéressait que trop peu d'étudiants par an, que ce soit en France ou en Allemagne.

Point sur la rentrée

140 candidatures ont été reçues en M1 dont 64 de l'étranger. C'est le double de l'an dernier.
50 ont été acceptés et 19 inscrits à ce jour. 1 Campus France vient d'avoir son visa et arrivera lundi. 2 autres n'ont toujours pas obtenu leur visa. C'est malheureusement classique.

En M2, il y avait 24 candidatures qui n'avaient pas fait le M1 crypto à Rennes. Là encore c'est plus que l'an dernier. 5 ont été acceptées et 3 sont venus, tous en parcours recherche car les prérequis sont importants pour le parcours classique et donc difficiles à rattraper.
Il y a finalement 16 étudiants inscrits dont 3 dans le parcours recherche. Il faut rajouter à cela 2 étudiants du double diplôme actuellement en Allemagne. Il y a également un étudiant Erasmus pour le premier semestre dans le parcours recherche.

L'emploi du temps a été compliqué à mettre en place à cause des contraintes sanitaires et notamment du fait que l'UFR maths et l'ISTIC n'ont pas mis en place les mêmes mesures. Il reste quelques bugs qu'on essaiera de résoudre au fur et à mesure.

DB propose de commencer le cours de crypto à base de code de S2 en décembre (2 cours et 2 TP sur la période où l'emploi du temps est quasi vide). Les étudiants en discutent ensemble et une décision sera prise avant fin octobre.

Point sur la situation sanitaire

Pour l'instant on tient en présentiel quasi-normal. Il n'est pas impossible que les conditions se durcissent un peu rapidement mais on va tenir aussi longtemps qu'on le pourra. Il y a une réunion à ce sujet à l'UFR mathématiques la semaine prochaine. La question des salles TP y sera notamment abordée. Beaucoup d'étudiants apportent leur propre ordinateur en M2 ce qui atténue le problème mais l'utilisation des claviers pose des problèmes sanitaires. Du gel est à disposition dans la salle. Il est également à priori possible d'apporter son propre clavier.

Composition de la commission

Christophe Ritzenthaler est parti de Rennes pour 4 ans, Patrick Derbez n'est jamais présent, Eric Gousset est parti de Rennes. Il semble plus opportun de les remplacer par des membres de l'équipe pédagogique. **SD** va demander à Mohamed Sabt (qui assure le cours de Network Security) et est impliqué dans le master Cyber. Benoit Gérard (qui assure le cours de sécurité des implémentations) pourra aussi être sollicité. C'est également important d'avoir un membre industriel. **PL** propose de demander à Marion Videau, responsable crypto de Quarkslab à Rennes. Si elle n'accepte pas on pourra solliciter des anciens du master à Amossys ou Secure-IC ou Olivier Sanders (Orange) qui aura un regard plus extérieur sur la formation.

Autre point

Déjà quelques retours des étudiants de M1 sur les nouveaux cours commun avec le master de cybersécurité sur le fait qu'ils ne partent pas de zéro, en particulier sur les questions de programmation. **SD** est en contact avec les responsables et les enseignants sur cette question pour améliorer les choses.