Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 2 février 2021

Présents: Romane Arvier (M2), Amélie Bru (M1), Delphine Boucher, Sylvain Duquesne, Pierre Loidreau, Elisa Lorenzo Garcia, Baptiste Mougeot (M1), Marion Videau.

Situation sanitaire et conséquences

Le premier semestre a commencé en présentiel et s'est terminé en distanciel. Le second semestre n'a malheureusement pas pu être avoir une part de présentiel (en dehors de quelques TP) et les semaines à venir n'incitent pas à l'optimiste. Le présentiel ne reprendra pas pour les M2 à part pour les CC qui ont tous été placés la dernière semaine de février.

Plusieurs étudiants ont beaucoup de difficultés avec ces conditions de travail. **SD** échange avec eux. Des solutions pour les étudiants qui décrochent peuvent être trouvées comme un étalement du M1 sur 2 ans. Dès qu'on pourra, on reprendra en présentiel.

AB : c'est très bien d'avoir des TP en présentiels même si tout le monde ne peut pas venir
SD : il ne faut pas hésiter à alerter les enseignants si les TP sont trop compliqués à suivre pour les étudiants qui restent à distance.
DB: Essaye de mettre en place les TP en présentiel. A également repéré des étudiants en difficulté. L'équipe pédagogique va plus échanger sur cette question.
AB : Tout le monde en a marre des cours à distance. Difficile de tenir 2h.
SD : l'UFR Maths encourage à faire des séances d'1h30. On ne l'a pas trop fait jusqu'à présent en M1 car il n'y a jamais 8h de cours dans la journée
RA/ELG : C'est passé à 1h30 en M2 sauf en codes correcteurs.
DB: certains étudiants de maths fondas ont 8h de cours. Essaye de faire moins de 2h, mais quand même pas 1h30. Pas trop pris de retard pour l'instant malgré çà.
SD : on va essayer de passer à 1h30 sans trop perdre sur le contenu.
BM : au-delà des cours enregistrés en vidéo, ce serait bien d'avoir des corrections des TD.
RA : demandeurs des vidéos en M2.
SD : ne pas hésiter à solliciter les enseignants si il manque des supports.

Bilan du premier semestre de M1

- **« Algorithmique de base »**
  BM : tout le monde est assez contents. Le distanciel s'est plutôt bien passé (y compris en TD avec un bon enseignant). Bases de Gröbner un peu rapides. DM sur les polynômes et contest appréciés.

- **« Algèbre de base »**
  AB : cours OK, mais pas de cours en distanciel, que des questions/réponses. Il fallait préparer les cours en avance → plus facile d'accumuler du retard. Les TD étaient biens.
  BM : plutôt positif sur le contenu.

- **« Probabilités pour la théorie de l'information»**
  AB : Tout le monde a apprécié, bien adapté même en distanciel. Problème d'emploi du temps un peu lourd (8h de proba en 2 jours).
  SD : Les emplois du temps ont été compliqués à faire, mais il ne faut pas hésiter à signaler ce type de problème très rapidement pour qu'on puisse essayer de les résoudre.

SD : Les 2 cours suivants sont des nouveaux cours de la Cyberschool, en anglais et communs avec le parcours de cybersécurité de l'ISTIC. Ils étaient censés repartir de 0 mais ont finalement posé de nombreux problèmes (y compris aux étudiants d'info).

- **« Low level programming »**
  BM : Au final, ceux qui n'ont pas décroché ont plutôt apprécié car ils ont appris à programmer et le principe du projet est motivant, çà force à avancer. Par contre plus de la moitié a décroché. Ca pourrait être utile d'avoir quelques heures supplémentaires en début d'année, éventuellement encadré par les M2, pour apprendre les bases utiles à ce module (Git par exemple). Système de notation démotivant (plusieurs étudiants voient mal l'intérêt de s'investir dans ce module avec des 0 au bout quelque soit le travail fourni).
  AB : handicapés par Git car il n'y avait pas d'explication et c'était du coup impossible d'envoyer son travail.
  RA : c'était déjà comme çà à Bordeaux et il n'a jamais voulu changer. Pour Git, il veut que les étudiants apprennent par eux mêmes.
  SD : même souci en cybersécurité. Des pistes ont déjà été évoquées comme une communication en réunion de rentrée pour éviter les décrochages ou des cours de remise à niveau début septembre (dans lesquelles on pourra intégrer Git)
  BM : pourquoi pas une aide aux devoirs par les M2.
  RA : les M2 n'ont pas du tout le temps. Le premier semestre est très chargé.
  SD : Pourquoi pas début septembre, c'est une bonne idée.

- **« Network Security »**
  AB : Appris beaucoup de choses mais pas de retour sur les problèmes rencontrés et les TP. Problème d'un étudiant qui n'est pas passé en Quizz.
  BM : bonne partie introductive aux réseaux. Bien tant que ca restait sur les aspects théoriques. Par contre la mise en pratique/concret a perdu beaucoup de monde à cause de la difficile prise en main des logiciels. Peut-être faudrait il passer à un seul logiciel. Notes pas représentatives de ce qui a été appris.
  AB : Pour le projet, la moitié des étudiants n'a pas réussi à installer le logiciel.
  SD : Pas encore clair ce qui se passera avec ce cours l'an prochain. On passera peut-être à un cours sans les aspects sécurité. Avec les aspects sécurité en M2.
  BM : L'enseignant a dit qu'il ne referait pas ce cours l'an prochain.
  AB : En ce qui concerne l'anglais, on s'en sort avec les diapos et en s'entraidant.
  BM : La langue n'est pas le plus gros obstacle dans ces cours.

- **« Anglais »**
  AB: Tout en présentiel. En demi-groupe pour tenir compte des contraintes COVID mais du coup 2 fois moins de cours.

- **« Histoire des maths »**
  AB : Ceux qui ne sont pas venus en présentiel ont fait le même sujet en distanciel avec un mois de délai → inégalitaire. Cours intéressant, mais ce sera bien d'avoir des maths un peu plus modernes.
  SD : On en tiendra compte en jury

- **Questions générales sur le M1**
  DB : est ce qu'on fait les CC en présentiel ou à distance ?
  SD : on espère pouvoir passer en distanciel avant la fin du semestre. En attendant, on fait soit du distanciel, soit on regroupe plusieurs CC au même moment.
  BM : ce serait mieux si il n'y avait pas eu de CC pendant les vacances pour pouvoir se reposer. Dommage qu'il n'y ait pas de lien avec la cryptographie dans les cours du S1.
  SD : problème récurrent. C'est une formation sur 2 ans et il faut d'abord poser les bases.
  BM : ca aurait été mieux de décaler un des 2 cours d'info car gros investissement.

- **« Semaine Profil »**
  RA : pas eu le temps et pas entendu parler.
  AB : tout le monde a participé mais difficile d'en tirer quelque chose.

Bilan du premier semestre de M2

RA : globalement trop chargé surtout avec le distanciel qui a impliqué beaucoup trop de choses à rendre. Il a fallu faire des choix et du coup certains modules ont été un peu laissés de côté. SIMP et SRES pourraient avoir lieu plus tôt dans la formation.
SD : difficile d'avancer sans les bases de crypto. Pour la sécurité réseaux, on a essayé cette année et ce n'était pas une grande réussite.
RA : problème d'incompatibilités d'emploi du temps pour les étudiants du parcours recherche. Y compris pour des examens.
SD : Il y a clairement eu des erreurs. On ne s'est pas méfié mais il y a eu cette année beaucoup plus de diversité de choix des étudiants de recherche. Protocole mis en place pour que ça ne se reproduise pas.
RA : Ce serait bien d'unifier un peu les outils de visio.
SD : Compliqué car plusieurs cours sont partagés avec d'autres formations. On a essayé avec Via en début de confinement mais du coup, il y avait trop de monde dessus et le service a saturé.
RA : Certains enseignants n'ont pas fait de cours mais juste fourni un poly en attendant les questions. Pas motivant.

- **« Courbes elliptiques pour la cryptographie »**
  RA : que du positif, TP très intéressants sur magma, bien guidés. Contest trop long car mord trop sur le S2.
  SD : c'était clairement trop long mais une fois annoncé, difficile de revenir en arrière.

- **« Programmation 1 (Java) »**
  RA : écart de niveau entre les TD avec les L3 (trop basique) et les TP (spécifiques crypto avec des librairies spéciales crypto pas facile à prendre en main). Enseignant très disponible et s'est bien adapté au distanciel. TP très intéressants mais un peu déconnectés des TD. Longs mais faisables.

- **« Réseaux euclidiens pour la cryptographie »**
  RA : retours très partagés. Preuves de sécurité intéressantes. Distanciel pas très bien géré. Examen un peu chaotique et grosses différences de traitement entre les étudiants.

- **« Sécurité réseaux »**
  RA : cours très intéressants mais trop de différence de niveau avec les étudiants de cybersécurité. L'enseignant a essayé de s'adapter mais trop de lacunes sur les bases en réseau.

- **« SIMP »**
  RA : très intéressant et très clair mais pas facile. L'enseignant est allé vite et a pas mal débordé car programme dense. TP pas bien adaptés au distanciel (utilise des boîtiers physique habituellement).

- **« C++ »**
  RA : très intéressant. CC à distance pas évident. Pas de TP à rendre → démotivant.

- **« GPU »**
  RA : plutôt intéressant. Partie GPU un peu trop rapide (pas de calcul pratique à cause de distanciel)

- **« Sécurité des données pour la propriété intellectuelle et la vie privée »**
  RA : Contenu très intéressant. Intervenants très biens.

- **« Protocoles de sécurité »**
  RA : que du CM. Slides pas faciles à relire, mais UE intéressante. Challenge bien mais demande beaucoup de travail. Pas assez d'indication pour installer les logiciels.
  SD : Ce serait bien de pouvoir accéder avec des machines virtuelles où tous ces logiciels (de M1 et de M2) sont installés → à voir avec cyberschool.

- « **Résolution de challenges de sécurité** »
  RA : Difficile. Gros écart de niveau avec les étudiants de cybersécurité. Très intéressant mais un peu déprimant quand on n'y arrive pas. Beaucoup de travail perso nécessaire. Pas beaucoup de crypto. Heureusement il y en avait un peu à la fin.

- **« Théorie de l'intersection »**
  RA : Cours assez compréhensible et clair, même si c'est difficile. Rythme soutenu. Déconcertant de ne pas avoir de TD.

Point sur les stages
SD : 3 étudiants n'ont pas encore trouvé de stage à ce jour.
PL : est ce que ça a été plus difficile que les autres années avec le Covid ?
RA : pas si difficile, il y avait pas mal d'offres. Surtout à partir de novembre.
SD : assez similaire à ce qui se passe d'habitude.
RA : y a t'il beaucoup de stages à l'étranger ?
SD : un seul (Suisse) mais c'est assez rare en général.

SD : A part **« Low level programming »** et **« Network security »** qui vont évoluer en M1, il n'y aura pas de gros changements l'an prochain. Il y en aura plus pour la rentrée 2022 puisqu'une nouvelle habilitation sera mise en place.