Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 28 janvier 2022

Présents (visio): Amélie Bru (M2), Delphine Boucher, Sylvain Duquesne, Emmanuel Fleury, Maël L'hostis (M1), Pierre Loidreau, Baptiste Mougeot (M2), Marion Videau.

Bilan du premier semestre de M2

BM : Le semestre s'est globalement bien passé. Retours plutôt positifs car plus de concret qu'en M1.
SD : Pas trop de surcharge de travail ?
BM : Pas spécialement, sauf pour certaines combinaisons d'UE (GPU et SED par exemple)

- **« Courbes elliptiques pour la cryptographie »**
  AB : 2 parties bien complémentaires et intéressantes. Dommage qu'il n'y ait pas de retour sur le dernier TP et sur le détail des notes. Pas assez d'implémentation de chiffrement basé sur les courbes (par rapport à la génération de courbes). Partie crypto de l'examen trop difficile
  SD : c'est vrai que l'examen était plus difficile que d'habitude. Non dit pendant la réunion : il a été noté sur 25 pour compenser.

- **« Programmation 1 (Java) »**
  AB : pourquoi c'est le plus gros coeff
  BM : matière sympa, il s'adapte au public. TP très bien
  SD : c'est là où il y a le plus d'heure et les coeffs/ECTS dépendent des heures. Les autres modules sont plus découpés. Dans la prochaine maquette tous les cours devraient être coeff 5
  AB : exam trop long et difficile d'éviter les petites erreurs à l'écrit

- **« Réseaux euclidiens pour la cryptographie »**
  AB : première partie théorique très difficile. L'enseignant s'en est rendu compte et essaiera de s'améliorer l'an prochain.
  BM : 2ème partie plus appliquée et bien appréciée. Ca manque de TP. Dommage qu'il y ait eu les 2 évaluations en même temps.
  EF : ce serait effectivement bien de faire des TP, avec sage par exemple.
  SD : On profitera des nouvelles maquettes pour en intégrer.

- **« Sécurité réseaux »**
  AB : cours très intéressant et beaucoup plus abordable que celui de M1. Pas mal de notions avaient déjà été vues l'an dernier. Heureusement que les TP étaient en présentiel
  BM : TP bien guidés et bien accompagnés par l'intervenant.
  SD : D'habitude ce module est compliqué. C'est bien si on arrive à le rendre plus abordable. Reste à trouver le bon équilibre entre ce qui est fait en M1 et en M2.
  AB : Dommage que c'était si condensé dans l'emploi du temps (8h par jour).
  SD : Difficile de gérer les intervenants extérieurs.

- **« C++ »**
  AB : Bien même si ca ne part pas de 0. Dommage qu'il n'y ait pas de projet. Un seul CC et TP pas notés → pas de moyen de se rattraper
  SD : Je ferai remonter car normalement, il faut au moins 2 notes

- **« GPU »**
  AB : plutôt intéressant mais trop de temps sur la partie programmation parallèle et très peu sur la partie GPU (basé sur les vidéos de l'an dernier mais clairement pas au point)
  BM : Pas vraiment de TP sur GPU.
  AB/BM : partie projet pas claire et grosse différence de traitement suivant les choix de sujet. Quelques problèmes de communication avec l'enseignante.

AB : Compliqué à gérer les TP et les projets car tous les PC n'ont pas de GPU dans la salle info.

- **« Sécurité des données pour la propriété intellectuelle et la vie privée »**
  AB : TB pour la culture mais compliqué et demande beaucoup d'investissement (lecture de code par exemple)

- **« Protocoles de sécurité »**
  AB : cours très intéressant, très théorique. Compliqué à suivre. Partie TP compliquée car languages pas connus avec peu d'aide. Projet compétitif entre les étudiants pas apprécié par tous mais ca oblige à s'investir que du CM.

- « **Résolution de challenges de sécurité** »
  AB : Difficile. Cours plus pensé pour les étudiants de cybersécurité.

- **« Parcours recherche »**
  BM : Peu de retour mais globalement intéressant. Pas mal de DM, durs mais ce n'est pas une surprise. Début de semestre un peu trop condensé

<u>Point sur les stages</u>
EF : Avez vous reçu assez de proposition ?
BM : Oui. Ceux qui n'ont pas trouvé n'ont pas eu de chance ou se sont mis à chercher tardivement
SD : 6 étudiants n'ont pas encore trouvé de stage à ce jour (3 en classique et 3 en recherche). Assez habituel mais compliqué car il commence à ne plus y avoir beaucoup d'offres. Ce n'est pas grave si le stage commence plus tard ou finit plus tard
BM : Dans ce dernier cas, faut il revenir à la fin du stage pour soutenir
SD : non, toutes les soutenances ont lieu en septembre et le diplôme est délivré dans la foulée même si le stage n'est pas terminé en pratique.
DB: condition 4 mois minimum ?
SD/EF : oui, mais c'est une contrainte purement pédagogique, on peut donc s'arranger.

EF : Début de retour sur Blockchain et SIMP ?
BM : Blockchain ça plaît beaucoup
RA : passage en distanciel pour SIMP → plus de difficultés avec les TP. Intéressant mais dur

<u>Bilan du premier semestre de M1</u>

ML : Globalement contents du master et du semestre. Tous ne savaient pas à quoi s'attendre. Semestre très chargé en terme de volume horaire alors que le S2 est beaucoup plus léger. Ce serait bien d'équilibrer un peu plus.
SD : Effectivement l'anglais est sur toute l'année et compte au S2, le projet de S2 ne rajoute pas d'heures dans l'emploi du temps et ca crée un déséquilibre
EF : Il y a des UE de S2 qui ont des prérequis → engorgement au S1

- **« Algorithmique de base »**
  ML : Cours bien. Examen terminal assez dur. Pourtant en TD, ça se passait bien.
  SD : Les notes ne sont effectivement pas bonnes. L'examen était peut-être long mais il y avait dedans des questions pas dures ou de cours pour lesquelles les réponses étaient en dessous des attentes. Reste à savoir si c'est un problème de compétences ou de temps disponible/stress
  ML : C'est vrai que la première partie de l'examen était assez perturbante
  DB: Et sur la partie TP ?
  ML : Ça a plutôt remonté les notes mais dommage que seul le dernier TP était noté.

- **« Algèbre de base »**
  ML : Vraiment dur, niveau recherche/ENS. Part assez vite et tout le monde n'a pas les bases du

L3 de Rennes. TD vraiment très bien. Il faut continuer à insister au moment des candidatures sur les prérequis à avoir pour ce cours (ANAR).
SD : Ca se passait mieux l'an dernier mais l'enseignant a changé. Les notes ne sont pas si mauvaises (moyenne de 9). TD spécifique pour le groupe crypto mis en place il y a quelques années → à garder.

- **« Probabilités pour la théorie de l'information»**
  ML : Peu de retours, pas de soucis particuliers. Intéressant.

- **« Low level programming »**
  ML : Demande beaucoup d'investissement mais on était prévenu. Certains ont du faire un choix entre ALGB/ALBA et LLP. Tout le monde en retire quand même quelque chose mais certains ont décroché.
  SD : les cours de remise à niveau ont ils été utiles.
  ML : Oui, très appréciable. Ce serait bien d'envoyer le cours d'Anne Canteaut en amont de la rentrée pour pouvoir s'avancer un peu.
  SD : Ca semble mieux que l'an dernier
  BM : plus d'étudiants se sont impliqués dans le module visiblement cette année
  AB : On les a encouragés à bien s'investir dans ce module
  SD/EF : Il y en a plus qui se sont investis que l'an dernier et ceux là ont mieux réussi. Les meilleurs du module sont même des crypto.

- **« Network Security »**
  SD : Module qui avait posé pas mal de problèmes l'an dernier. L'enseignant a changé et le programme a été recentré sur les bases du réseau et moins sur la sécurité.
  ML : Clairement mieux mais les cyber ont toujours un meilleur bagage. L'enseignant a fait des efforts mais ne réalise pas forcément que les étudiants de crypto partent de rien. Ça s'est particulièrement vu sur certains TP que l'enseignant pensait triviaux alors que ça a demandé pas mal d'investissement. Ca reste une UE compliquée mais intéressante. Gros décalage entre les 2 populations.
  BM : Ce recentrage, c'est bien, car il y avait beaucoup d'intersection entre le cours de l'an dernier et le cours de M2. Ca va dans le bon sens.

DB : Beaucoup d'étudiants en COCO et en particulier en TD en amphi. Comment le ressentez vous
ML : C'est sûr que ce serait mieux d'avoir un TD séparé. Mais personne ne s'en est plaint
DB: N'hésitez pas à le dire si vous en ressentez le besoin

<u>Prochaine maquette du master</u>
SD :

- Mise en place à la rentrée 2023.
- Rien d'acté pour le moment mais ça va aller vite. Idée de passer tous les modules à 5 ECTS ce qui simplifiera les mises en commun de module avec les autres parcours, en particulier cybersécurité. Possibilité également de modules sur des demi-semestres ce qui pourra répondre aux questions de prérequis. Par exemple, ALGB pourrait être coupé en 2 modules et seul le premier pourrait être suivi dans le master crypto. Il faudra quand même
- Problème du départ à la retraite de Mr Petritis qui assure 3 cours pour lesquels on a pas forcément les compétences à l'UFR Maths pour prendre la relève (surtout pour le cours de cryptographie quantique)
- Faut il introduire des choix en M1 (dans la maquette actuelle, il n'y en a aucun) ou rester sur un tronc commun

BM : Pourquoi pas pour ceux qui veulent faire plutôt les aspects maths.
DB: Attention parce que ca va ouvrir les portes du parcours recherche et il y a peu de débouchés et c'est compliqué d'avoir des bourses de thèse.
SD : Je confirme : un étudiant qui veut faire le parcours recherche devrait faire le M1 maths fondas avec

CRYP et COCO en option. Ce parcours n'a pas vocation à accueillir plus d'un ou 2 étudiants par an et qui feront une thèse dans un labo de maths ensuite. Le parcours classique est tout à fait adapté pour faire une thèse académique ou industrielle en cryptographie
AB : On ne sait pas forcément où on va aller en arrivant en M1. Ça peut être dommage de faire des choix qui ferment des portes sans vraiment savoir.
BM : attention aussi aux prérequis.
ML : Pas gênant d'avoir un tronc commun en S1 qui permet de découvrir les différents aspects
AB : Pourquoi pas basculer des options du M2 (car il y en a beaucoup) en M1
DB: Plus sûr pour les étudiants d'avoir quelque chose de bien cadré au début
EF : OK, pourquoi pas quelques chois au S2

Points divers
BM : pas mal de cas positifs et de cas contacts. Ce serait bien d'avoir plus de ressources en ligne pour pouvoir rattraper plus facilement.
SD/DB : oui, bien sûr, on peut faire des choses, il faut penser à nous solliciter en cas de besoin.
ML : OK, mais il y a déjà pas mal de choses.
SD : en cas d'absence à une épreuve, il y a droit à une épreuve de substitution. Pareil, il faut solliciter les enseignants et ils seront ouverts et compréhensifs.