Compte rendu de la réunion du conseil de parcours du Master de cryptographie du 7 février 2024

Présents: Delphine Boucher, Sylvain Duquesne, Mathieu Goessens, Pierre Loidreau, Alban Perreaux (M1), Marion Videau (visio), Romain Vovard (M2)

Remarques générales sur cette réunion :

- éviter les acronymes de cours et préciser les intervenants
- les retours/avis/suggestions émises pendant ce conseil seront remontées aux enseignants

Bilan du premier semestre de M1

SD : Effectif de 25 étudiants cette année. 17 devraient valider leur S1 ou en être très près. 2 sont dans une situation un peu particulière. Les 6 autres sont en difficulté mais pas insurmontable (au dessus de 8 de moyenne). J'en ai déjà reçu 2 et je prévois de recevoir les autres rapidement.
AP : En début de semestre, les étudiants ont eu du mal à comprendre le lien avec la crypto, car la formation reste très générale. Mais vite compris l'importance des cours proposés (remise à niveau en info, bases de l'algèbre). Quelques semaines d'octobre un peu tendues mais semestre globalement équilibré en terme de charge de travail. Reste ponctuellement quelques points à améliorer.
SD : Le rééquilibrage de la charge de travail entre les semestres était l'objectif principal de la nouvelle version du master. C'est très bien que ça se concrétise en pratique.

- **« Algorithmique de base »**
  AP : 3 enseignants avec une impression de manque de communication entre eux en particulier pour les TD d'arithmétique pour lesquels l'enseignant de TD semblait un peu perdu. Trop peu de communication également sur le système de notation. Il faudrait connaître le poids des différents CC dès le début. Le contenu des cours et les TP étaient biens, demandaient un peu de travail supplémentaire pour les terminer mais çà restait raisonnable.
  SD : On essaiera de mieux communiquer à l'avenir sur les modalités de notation.
  DB: C'est vrai qu'il faudrait faire quelque chose pour la cohérence de ce module. On s'arrange tous les ans pour trouver des intervenants avec les compétences nécessaires, mais ce serait plus adapté de confier le cours à une seule personne. Pour l'instant, on a personne avec ce profil mais çà pourrait évoluer l'an prochain. Pensez vous qu'il vaut mieux laisser les résultants à la fin ou les faire dans la foulée des polynômes ?
  AP : C'est mieux dans la foulée sinon ça parait déconnecté et ce qui est fait entre temps (tri, graphes, arithmétique) n'apporte rien à la compréhension des résultants.

- **« Algèbre de base »**
  SD : allégé par rapport à l'an dernier (passage de 8 à 5 ECTS)
  AP : TB autant en CM qu'en TD. Enseignants à l'écoute des retours faits au fil du semestre. Pas perturbant d'être avec les MFA en CM. TP très bien aussi et permettaient d'approfondir. Programme assez chargé et du coup très rapide à la fin sur les extensions de corps finis alors que c'est le plus utile pour nous. Difficile en COCO ce semestre par exemple.
  DB: en COCO, on attend surtout de vous sur les aspects manipulation des corps et de leurs extensions et algorithmiques/calculatoires.

- **« Outils de probabilités et statistiques »**
  AP : très rapide, très dense. Pas assez de temps sur les statistiques. TP encore perfectibles. Par exemple, pas de rendu de TP obligatoire donc moins motivant pour s'y investir. Enseignante à l'écoute et s'adapte.
  Peut etre trop de temps sur les rappels de probabilité de base en septembre mais tout le monde n'a pas les mêmes prérequis
  MG : Est ce que les TP sont obligatoires comme en info ?
  SD : C'est laissé à l'appréciation des enseignants, on est pris entre la nécessaire

responsabilisation des étudiants et la réalité d'un moindre investissement sans contrainte (surtout avec d'autres contraintes dans les autres modules).

- **« Théorie de l'information »**
  AP : CM et poly TB, contenu intéressant, très cadré, mais TD très éloignés du CM et CC sans rapport avec ce qui est fait en TD. En particulier, dernier CC catastrophique pour tout le monde. Par contre c'était bien que ce soit tassé en début d'année car ça a permis de dégager du temps en novembre/décembre pour les projets d'informatique. Chaînes de Markov faites avant de les faire en proba.
  SD/PL : dommage de ne pas avoir une meilleure articulation entre ce cours et OPS. Mais on garde quand même le principe de concentrer ce cours en début de semestre.

- **« Low level programming »**
  AP : Répartition CM/TP catastrophique (d'abord tous les CM et ensuite tous les TP). En plus les CM consistaient essentiellement en de la lecture de doc et manquaient d'exemples et de pratique. Une remise à niveau comme initialement annoncée aurait été bien pour apprendre l'environnement (git, …) et éviter de perdre un mois sur le TP1 pourtant très basique → retard accumulé (d'autant plus qu'il n'y a pas de deadline pour rendre les TP). Du coup, pas eu le temps de finir le projet, ce qui est dommage, que ce soit pour la note ou pour le contenu. La plupart des étudiants ont eu un déclic en novembre. Pas le sentiment de maîtriser le C mais au moins les bases sont connues.
  MG : L'ISTIC n'a pas voulu mettre en place de remise à niveau car pas de crédits ECTS associés. Mais avec le recul, l'ISTIC s'est laissé convaincre de revenir sur cette décision. Ce serait mieux que l'enseignante de CM assure les TP de crypto plutôt que ceux de cyber qui ont moins besoin d'aide au début. Il est envisagé que ce cours soit donné en anglais à l'avenir pour s'ouvrir aux parcours internationaux, mais je ne suis pas sûr que l'enseignante souhaite rajouter une couche de complexité.

- **« Analyse et conception formelle »**
  AP : Contenu très intéressant, retour très positif. CM, TD, TP très bien construits. Le seul hic, c'est qu'aucune information n'a été donnée sur le mode de calcul de la note finale.
  SD : C'est important que les notes intermédiaires soient communiquées aux étudiants, mais ça ne pose pas de problème à certains étudiants que les notes soient diffusées ouvertement sur Moodle.
  AP : Ca gène effectivement certains étudiants mais la majorité préfère avoir sa note.
  MG : On peut utiliser les numéros d'étudiants. C'est pas anonyme, mais l'info n'est pas disponible immédiatement.

- **« Anglais »**
  AP : TB, pas grand-chose à redire. Cours vivants avec beaucoup de pratique.

<u>Bilan du premier semestre de M2</u>
SD : 26 étudiants mais pas de résultat semestriel pour le moment. 2 étudiants ont plus ou moins abandonné pas en raison de leurs résultats.

- **« Courbes elliptiques en cryptographie »**
  RV : Partie théorique démarrée trop fort et trop vite: enseignant mal informé sur les connaissances antérieures des étudiants, pas de séance de TD, juste quelques exercices intégrés au cours. Après échanges avec l'enseignant, il est passé à du cours en autonomie avec possibilité de le solliciter. Au final, contenu mal compris. Partie cryptographie très bien.

- **« Réseaux euclidiens en cryptographie »**
  RV : cours de la partie théorique un peu rapide mais très bien, par contre enseignante de TD pas à la hauteur, heureusement des corrections ont été postées en ligne par l'enseignant de CM. Un seul TP mais pas intéressant/utile.

Seconde partie du cours très bien, avec une fiche de rappel appréciée. TD bien faits mais ça aurait été mieux d'avoir les feuilles en avance pour éviter les blancs pendant les séances. Souvent beaucoup de retard à la fin des TD.
CC peu apprécié car rien à voir avec les TD, plutôt de la culture générale sur les réductions.

- **« Sécurité réseaux »**
  RV : concentré sur 2 semaines, c'est vraiment pas terrible. Cours intéressant et bon enseignant mais pas grand-chose de nouveau par rapport au cours de réseaux de M1. TP trop condensés pour que ça apporte. Mais pas mal d'aide du prof et le cours de l'an dernier a bien aidé.
  MG : Le cours de M1 a été conçu pour rendre le cours de M2 presque optionnel car SRES est optionnel en M2 cyber et ils ont besoin de voir un certain nombre de choses.
  Les TP de SRES sont assez peu guidés et du coup il ne vont pas très loin. Probablement des choses à améliorer sur les sujets de TP.
  SD : On peut rendre le cours optionnel l'an prochain, mais ce serait mieux de rééquilibrer les 2 modules. Comme le cours de M1 n'est pas au même semestre pour les cyber et les crypto, une solution serait d'enlever quelques points en crypto

- **« Cryptanalyse »**
  RV : partie asymétrique sans intérêt, peu voire rien appris par rapport au cours de cryptographie de M1. Évaluation avec cryptohack ou rootme. TP trop vagues ou pas assez guidés. Pas réussi à les faire et peu d'aide de l'enseignante.
  Partie symétrique très intéressante et bien faite mais intense, pas assez de temps. Ce serait bien que cette partie soit plus longue. Plutôt négatif par contre pour les TP, difficiles, demandent beaucoup de puissance de calcul et avec peu de temps pour les rendre.
  SD : C'est ennuyant pour la partie asymétrique, mais c'est probable que les étudiants de cyber eux y apprennent des choses.
  MG : pourquoi pas dispenser les crypto de cette partie du cours.

- **« Sécurité des implémentations »**
  RV : Première partie intéressante (boite blanche, boite noire) mais évaluation plus difficile qu'attendu par l'enseignant. TP très intéressants sur Raspberry.
  Deuxième partie intéressante également (side channel) mais mal structurée, manque d'explications pour comprendre comment ca marche. TP sympa mais avec quelques erreurs et des problèmes d'organisation qui ont entraîné des pertes de temps, pas bien guidés.
  MG : L'enseignant sera preneur de ces retours pour améliorer l'an prochain, n'hésitez pas à faire remonter

- **« Anglais »**
  RV : bien, rien à redire, effectivement on parle, mais critères de notation pas très compréhensibles

- **« Programmation objet, Java »**
  RV : problèmes rencontrés avec l'enseignant (cours en 30mn). Projet pas adapté (Signal amélioré) à ce qui a été fait en TP (basiques, mal préparés par l'enseignant et pas orienté crypto) et donné trop tard dans le semestre. Pas une bonne expérience au final. Avis général plutôt pour le rendre optionnel voire le supprimer
  MG : Attention, le java c'est quand même très largement utilisé en entreprise
  MV : Nous on n'utilise pas Java mais on en trouve beaucoup dans les produits qu'on doit évaluer.
  SD : est-ce dur de s'adapter de C++ à Java ?
  MG : non, mais l'absence de Java dans un CV peut être considéré comme éliminatoire par des RH
  SD : La question de la place de ce module dans le master reste en suspens car on ne sait pas comment va évoluer C++ l'an prochain (l'enseignant part à la retraite).

« C++ »
RV : TB. Beaucoup plus apprécié que Java, tout va très bien

« Sécurité des protocoles »
RV : peu de retour mais globalement apprécié, sauf sur le contenu de l'examen. Challenge intéressant.

« Preuves de sécurité »
RV : très intéressant. Ca aurait été mieux de l'avoir avant REC (surtout la deuxième partie). Mais énoncés des CC beaucoup trop compliqués, pas clairs et ambigus. TD très intéressants et bien faits. Partie symétrique trop semblable à la partie asymétrique (dès qu'on remplace l'AES par un oracle, c'est globalement la même chose).
SD : La question se pose de le passer en obligatoire, mais ça peut se faire facilement au moment de la réunion de rentrée. A voir avec les autres formations concernées si on peut l'avancer dans le semestre.

« Programmation parallèle et sur GPU »
RV : cours apprécié, bien structuré bien mais porte plus sur le parallélisme/calcul distribué que les GPU. Dommage qu'il n'y ait pas de correction pour les TP. Réponses aux questions peu adaptées. Projet intéressant.

« Advanced Hardware Protection »
RV : pas assez de bases en micro-architecture. Intense car emploi du temps très serré. Dense et dur mais très intéressant. Difficulté des TP exponentielle et surtout tout de suite dans la foulée des cours, pas le temps de digérer. Même les étudiants du parcours cyber/hardware ont du mal à suivre.
MG : les étudiants de cyber ont un cours de hardware en M1, ce serait bien que les crypto aient au moins une introduction.
SD : si tous les étudiants sont en difficultés, il faudrait aussi que l'enseignant adapte le niveau et passe un peu plus de temps sur les prérequis.
RV : ce serait effectivement bien d'avoir un cours de micro-architecture de base en M1. Il y en a besoin dans pas mal de stages, dans l'embarqué.
SD : c'est vrai que c'est très utile et que c'est nécessaire d'avoir les bases pour pouvoir échanger avec les spécialistes du domaine. Mais ce ne sont pas des compétences que les entreprises recherche chez les diplômés de ce master.

« Blockchain »
RV : trop condensé dans l'emploi du temps et avec trois intervenants. Une partie des cours en anglais mais la marche est trop haute alors que c'était la partie à priori la plus intéressante. Le reste c'est plus de la culture générale. Assez mitigé au final.
MG : Il ne faut pas perdre de vue que des attaques pourtant très simples marchent encore sur beaucoup de produits commercialisés. Donc même la culture générale permet de répondre à des problématiques industrielles d'actualité.

RV : Problème de compréhension en théorie algorithmique des nombres car peu d'arguments écrits, beaucoup d'oral. Il y a un support de cours mais difficile de suivre et de voir où il veut aller dans ses arguments.
DB : Il faut en parler directement à l'enseignant. Il sera preneur d'avis/retours et s'adaptera.

<u>Point sur les stages</u>

SD : 6 n'ont pas encore trouvé de stage. C'est classique à cette période de l'année. Ce n'est pas pas spécialement inquiétant (il reste 8 mois pour effectuer un stage de 4 mois) mais stressant pour les étudiants concernés d'autant plus que les offres de stages sont plus rares.

MG : Si certains étudiants ont besoin d'un coup de main pour leur CV ou leur lettre de motivation, il ne faut pas hésiter à nous solliciter.

RV : Tous ceux qui ont trouvé un stage sont contents du sujet. Certains ont rencontré quelques difficultés dans la recherche, essentiellement des baisses de moral/motivation en cas de réponses négatives et des entretiens qui tombaient mal par rapport à la charge de travail à ce moment là.

Place des femmes dans la formation

MV : comment faire pour attirer plus de femmes dans la formation et donc dans la profession ?
SD : jusqu'à présent, les promotions étaient relativement équilibrées (entre 30 et 40 % de femmes). La promo de M1 de cette année est largement en dessous (5 étudiantes sur une promo de 25) et même en dessous du taux de candidatures (27%) mais avec beaucoup de dossiers de candidatures très clairement en retrait, voire hors profil. A voir l'an prochain si c'était un accident ou si c'est une tendance de fond
MV : conséquence du COVID ou de l'introduction des spécialités au lycée par exemple ?
MG : en cyber et plus généralement en info, c'est encore pire. Autour de 10 % en général alors que c'est plus mixte en licence.
AP : ca se ressent dans la promo, mais elles sont malgré tout bien intégrées.