Compte rendu de la réunion du conseil de parcours du Master de cryptographie du 26 septembre 2023

Présents: Delphine Boucher, Sylvain Duquesne, Mathieu Goessens, Pierre Loidreau (en visio), Maël L'hostis (M2, en visio), Tanguy Medevielle (M2), Romain Vovard (M1 l'an dernier)
Absente : Marion Videau

Suite au départ d'Emmanuel Fleury à Bordeaux, Mathieu Goessens intègre le conseil de parcours comme représentant de l'ISTIC et de la cyberschool.

Bilan du second semestre de M1

RV : Assez pauvre en matière, moins de travail qu'au premier semestre. Gros déséquilibre entre les 2 semestres. Pas mal d'entraide dans la promo.
SD : Ca confirme ce qui avait bien été identifié au moment du bilan du premier semestre. Ca a été normalement corrigé dans la nouvelle maquette.

- « Codes correcteurs»
  RV : Très bons retours sauf sur l'intervenant d'un des groupes de TD. Un retour sur une trop grande importance du quiz dans la note finale
- « Cryptographie»
  RV : Bons retours sur le cours, stimulant. Dommage que les slides soient tantôt en anglais tantôt en français. Soucis avec l'enseignante de TD. Corrections pas terribles. Dommage de ne pas avoir le détail des notes (pas de retour sur les TP et sur l'AES).
  SD : effectivement, ce n'est pas normal. Je le mettrai sur Moodle désormais
- « Machine learning »
  RV : Assez inintéressant. Beaucoup de copier/coller pendant les TP. La 2ème partie du cours est mieux mais globalement trop survolé pour comprendre les maths derrière. Motivations peu visibles.
- « Complexité»
  RV : Globalement apprécié. Rythme un peu lent mais abordable. Pas assez de temps passé sur la complexité en elle-même qui est reléguée tout à la fin. Un peu trop orienté langage/logique.
- « Anglais»
  RV : Rien de nouveau par rapport au S1. Toujours beaucoup d'investissement demandé.
- « Projet tutoré»
  RV : Satisfaisant de mener à bien un projet, mais pas du tout tutoré.
  SD : Tout le temps comme çà. Je suis réactif en cas de sollicitation mais il y en a très peu en pratique. Le mot « tutoré » a d'ailleurs été supprimé dans la nouvelle maquette. Ceci dit l'idée proposée par **MG** de demander un petit point d'étape mi mai est bonne et sera mise en place dès cette année.
  RV : Problème de plusieurs étudiants qui se sont retrouvés à travailler seul sur le projet
  SD : Le problème a effectivement été identifié et malheureusement il est difficile d'y répondre une fois que les binômes constitués ont commencé à travailler. Ca fait partie du travail en équipe et on retrouve ce genre de situation dans la vie professionnelle. Il en a été tenu compte dans la notation mais ca ne résout pas les difficultés rencontrées par les étudiants concernés.
- « Rencontres de professionnels »
  RV : entreprises plus intéressantes présentées ce semestre. Information toujours pas terrible pour savoir si on est concernés ou pas.
  MG : pour l'instant personne pour reprendre çà (la personne qui s'en occupait a quitté la cyberschool). J'en organise quelques unes mais sur le créneau de SIMP pour l'instant. On va essayer de changer. Si vous avez des suggestions, n'hésitez pas.

SD : 25 étudiants ont validé l'année et 8 n'ont pas validé, souvent avec des conditions d'études difficiles. On note malgré tout moins de décrochages que les années précédentes ce qui confirme qu'il y a eu un effet post-covid.

Bilan du second semestre de M2

TM/ML : Bilan plutot positif du semestre 2 et de l'année en général. Arrivée en stage avec de bonnes bases. Année assez difficile, beaucoup de travail mais impression d'avoir beaucoup appris. Manque de communication au sein de certaines équipes pédagogiques (REC par exemple). Problèmes d'emploi du temps (certaines options concentrées sur quelques semaines, SRES par exemple)
SD : C'est à cause des intervenants extérieurs, en particulier industriels. C'est bien de les avoir mais ca rejoute des contraintes fortes sur les emplois du temps. C'est pareil cette année.
MG : pas assez guidé pour les TP de SRES (enseignant informé), je vous redirai un peu avant en vous donnant des refs/Mooc pour anticiper

- « Théorie algorithmique des nombres pour la cryptographie »
  TM : Très satisfaisant, TP appréciés. Bien équilibré, bon enseignant.
- « Codes correcteurs en cryptographie» :
  TM : Globalement satisfaisant et intéressant pour la première partie du cours. Seconde partie moins claire et communication difficile pour la partie DM. Module trop étalé entre les 2 parties
  DB: C'est en grande partie du au départ d'une des intervenantes, il n'y aura plus qu'une seule partie cette année.
- « Cryptographie quantique »
  TM : Prof bien, mais contenu moyennement apprécié. Lien avec la cryptographie quantique arrive très tardivement. Très orienté maths et pas évident/motivant à suivre.
  SD : On profite du second semestre pour faire un peu plus de maths et de théorique qui ont moins d'impact sur la recherche de stages. C'est donc normal que ce semestre soit plus orienté dans ce sens. Pour autant, le lien avec le coeur de la formation devrait bien rester présent pendant tout le semestre.
- Cours du parcours recherche
  TM : Pas vraiment utile pour la crypto, trop théorique. Sauf peut-être surfaces de Riemann. Cours compliqués à suivre.
  SD : C'est vrai et il n'y a pas d'ambiguïté puisque les étudiants concernés sont systématiquement prévenus avant d'intégrer la formation. Il faut voir ce parcours comme mi-crypto, mi- maths fondas.
- « Cryptanalyse »
  ML : Plutot satisfaisant, mais dispensé rapidement et assez dense. Format challenge des TP apprécié.
- « Blockchain ».
  ML : Très satisfaisant. Permet de voir des aspects de la crypto dans le monde réel. Partie théorique un peu poussive mais partie pratique très intéressante.
- « Preuves de sécurité »
  ML : Très satisfaisant, mais assez difficile. Concepts qui auraient pu servir plus tôt voire qui sont considérés comme prérequis (réseaux euclidiens par exemple)
  SD : C'est pour çà qu'on a introduit ce cours mais effectivement, ce serait plus logique de le faire plus tôt dans la formation. Nous y réfléchirons pour la suite. Mais on est un peu coincés car il est important que réseaux euclidiens arrive tôt dans l'année pour la recherche de stage
  TM : Au pire, couper en réseaux euclidiens en 2 en faisant la partie intro/protocoles rapidement et la partie preuves plus tard dans l'année
- « Anglais » :
  ML : pas de retour, mais ca s'est globalement bien passé

Bilan des stages de M2
TM/ML : Trop peu de retour sur les stages pour être représentatif.
SD : Encore une fois, les retours des entreprises sur les stages sont globalement positifs. Malgré une grosse promo la plupart des étudiants a trouvé assez facilement un stage. Il y avait 24 étudiants inscrits plus un encore en double diplôme avec Karlsruhe. 23 ont validé l'année, 1 redouble et 1 a trouvé un

emploi après son stage sans avoir validé le M2. A ce jour et à ma connaissance, 15 d'entre eux ont trouvé un emploi ou une thèse (9). C'est similaire aux années antérieures, sauf pour les thèses où il y a eu beaucoup d'offres cette année en raison du PEPR sécurité. Il faut s'attendre à ce que ça continue.

Point sur la rentrée

SD : Quasiment autant de candidatures en M1 cette année que l'an dernier (166 contre 177 l'an dernier) pour seulement une vingtaine de places car la promo de l'an dernier était trop importante et il y a 4 redoublants. Limiter la promo à 24 permet de tourner avec un seul groupe de TP. Il y avait 33 candidatures Campus France. 3 ont été retenues mais aucun n'est venu. Les problèmes se multipliant avec Campus France, la formation n'y sera plus proposée l'an prochain.
La promotion de cette année comporte 24 étudiants dont seulement 5 femmes. C'est cohérent avec la proportion de candidates mais peu par rapport aux années précédentes (un bon tiers). Il faudra surveiller l'évolution.
DB : C'est pareil en prépa agreg
MG : Il faudrait comparer avec les autres M1 de maths et la filière scientifique en général. Peut-être un premier effet de la désaffection des filles pour les maths au lycée.

La spécificité de l'année est en effet la mise en place de la plateforme monmaster sur le modèle de parcours sup. Les conséquences pratiques sont les suivantes (à confirmer à l'usage)

- Origine des étudiants inscrits moins variée (essentiellement Bretagne/Centre/Pays de la Loire)
- Globalement plus simple à gérer malgré quelques problèmes techniques
- Moins de réponses positives (Le 70eme classé a été pris à l'issu de la procédure cette année contre le 48eme l'an dernier pour moins de places)
- Moins de désistement de dernière minute (effectif stable fin juin/début juillet)

SD : En M2, il y avait 32 candidatures qui n'avaient pas fait le M1 crypto à Rennes et une seule admise dans le parcours recherche car les prérequis sont importants pour le parcours classique et donc difficiles à rattraper. Il y a finalement 26 étudiants inscrits.

La rentrée a été marquée par des difficultés importantes dans la mise en place des emplois du temps (chevauchements de cours, journées sans pause méridionale ou 8h-18h sans arrêt en fonction des choix d'option). Essentiellement en raison de la nouvelle maquette et d'un manque de coordination avec l'ISTIC.
MG : Manque une des personnes qui gère les emplois du temps à l'ISTIC
SD : Il y a aussi eu un problème pour trouver un intervenant pour Java. La question se posera l'an prochain si on conserve ce cours ou si on rend C++ obligatoire à la place (mais changement d'enseignant de C++ à prévoir)

RV : Cours de courbes elliptiques trop dur à suivre et trop rapide. L'enseignant considère trop de prérequis de maths fondas. Pas de feuilles de TD. Les étudiants utilisent le cours de l'an dernier qui heureusement est bien fait.
DB/SD : C'est un enseignant qui vient d'arriver à Rennes. Nous l'avons briefé sur le niveau attendu et les bases qui pouvaient être considérées comme acquises. On va en reparler avec lui pour qu'il s'adapte mieux au public visé. La seconde partie du cours ne sera pas impactée car elle est assez indépendante.