Compte rendu de la réunion du conseil de parcours du Master de cryptographie du 1er octobre 2024

Présents: Delphine Boucher, Sylvain Duquesne, Mathieu Goessens, Alban Perreaux (M2), Romain Vovard (M2 l'an dernier, en visio)
Absents excusés : Pierre Loidreau, Marion Videau

Bilan du second semestre de M1

AP : le second semestre a été largement mieux appréhendé et apprécié que le premier, il répondait beaucoup plus attentes.
SD : c'est tout à fait logique. Le premier semestre est important pour poser les bases mais est thématiquement assez peu marqué. Suite aux discussions de ce conseil, un gros travail a été fait l'an dernier pour rééquilibrer la charge de travail entre les 2 semestres et il semble avoir porté ses fruits.
AP : globalement sur les cours de second semestre avec des aspects pratiques, ce serait bien d'avoir plus de retour sur certaines implémentations (au-delà de la note). Par forcément sur les premiers TP plus faciles mais sur les projets et les derniers TP un peu plus longs et délicats.
MG : une solution est d'identifier les erreurs/écueils les plus importants et d'utiliser une séance de TD ou de TP pour faire le point dessus.
AP : sur l'année, on retient une bonne cohérence de la formation avec le projet professionnel (3/4 des étudiants ont répondu au questionnaire).

- « Codes correcteurs»
  AP : très bons retours, contenu du cours et TP très intéressants malgré quelques difficultés pour s'adapter à la méthode de travail d'un des enseignants et un peu de frustration que les aspects crypto ne soient abordés qu'à la toute fin.
- « Cryptographie»
  AP : très bons retours aussi. Rythme trop lent au début sur les aspects faciles du module. Pourquoi pas réduire le nombre de CM du début pour augmenter les aspects pratiques. Ce serait bien aussi que les TP/projets soient plus pris en compte dans la note finale.
  SD : pas trivial de transformer les cours en TP dès cette année, mais on pourrait déjà plus densifier les cours en début de semestre pour que les TP/projets arrivent plus tôt et avec un emploi du temps plus allégé en fin de semestre.
- « Compléments en cryptographie»
  AP : quelques personnes n'arrivaient pas à différencier les 2 cours de crypto.
  SD : c'est normal, c'est fait pour. La scission ne sert qu'à pouvoir proposer le premier cours en maths fondas. C'est plus compliqué pour les étudiants de maths fondas, il faut qu'on s'améliore sur la communication.
  AP : il faudrait annoncer le projet un peu plus tôt car le rythme est globalement lent en début de semestre et les étudiants ne voient pas bien venir l'intensification du travail à fournir avec la multiplication des notions plus compliquées, des TP à rendre et des projets.
- « Complexité»
  AP : impeccable, rien à redire, contenu très bien, bien équilibré entre les thématiques. Petit coup de mou en mars car c'est un petit module donc un peu trop étalé. Peut-être aussi bien de le tasser en début de semestre.
  SD : c'est une bonne idée et ça répondra en même temps à la problématique du rythme inconstant du semestre déjà évoqué.
- « Network Security »
  AP : cours bien, charge de travail un peu élevée sur les TP au début mais l'enseignant avait prévenu. Ce serait pas mal que la salle soit accessible pour pouvoir travailler ensemble sur les TP en dehors des séances.

MG : c'est un accès par badge car il y a du matériel dedans mais c'est envisageable d'avoir un accès et on va s'en occuper.
DB : avez vous eu des cours en anglais et est-ce que ça pose problème ?
AP : un seul mais c'est très bien et il ressort des premières discussions avec les M1 que l'anglais n'est pas un obstacle en ALBA cette année.

- « Apprentissage statistique » cours optionnel
  AP : le courant n'est pas passé avec l'enseignant et ses méthodes pédagogiques. Cours beaucoup trop orientés théorique alors qu'elle ne servait même pas en TP/projet/évaluation. Finalement, très peu d'étudiants présents. Ceci dit, sur le fond c'est intéressant et pas trop dur à valider (le projet est déconnecté des cours).
  SD : les CSM ont aussi trouvé trop dure la partie théorique. Le responsable du M1 CSM a déjà fait remonter à l'enseignant mais je ferai de même.
- « Théorie des nombres » cours optionnel
  AP : retour très positif, contenu très intéressant, mais cours difficile à valider.
- « Algèbre commutative et géométrie algébrique » cours optionnel
  AP : même retours que théorie des nombres, beaucoup de théorie et pas le temps de s'y impliquer autant qu'il faudrait.
  SD/DB : ce sont des cours de S2 de maths fondas et donc naturellement plus difficiles et avec un public plus théorique et de niveau plus élevé (cours suivis par les étudiants de l'ENS). Les enseignants s'adaptent et avancent plus vite et plus loin.
- « Histoire des maths » cours optionnel
  AP : pas de retour détaillé.
- « Projet»
  AP : très bien sur la liberté des sujets, le travail en binôme, de pouvoir assister à toutes les soutenances. Certains étudiants ont mal reparti leur charge de travail dans le semestre et le projet surcharge pas mal la fin de semestre. Ce serait bien d'avoir une fiche récapitulative des attendus et des dates butoirs. Plusieurs étudiants auraient aimé avoir un retour sur leur projet et leur présentation.
  SD : le but est de laisser le plus de temps possible pour ces projets et on ne connaît la date du jury qu'en fin de semestre, donc difficile de s'avancer sur les dates butoirs tôt mais c'est une bonne idée de faire une fiche. La question d'un retour est tout à fait légitime et j'ai répondu aux étudiants qui me l'ont demandé, mais c'est vrai que comme les soutenances ont lieu au dernier moment, cette étape de débriefing passe facilement à la trappe.

SD : 19 étudiants ont validé l'année et 6 n'ont pas validé. Parmi ces 6 étudiants, 2 étaient déjà redoublants, 1 était en Erasmus et a plus suivi le parcours maths fondas que crypto et 1 est arrivé en cours d'année avec déjà un M1 validé. Le contrat était donc uniquement de valider le second semestre, ce qu'il a fait. Enfin, un étudiant a choisi de changer de voie car la formation ne répondait pas à ses attentes et un redouble.

<u>Bilan du second semestre de M2</u>

RV : seulement 3 matières officiellement. Malgré tout assez intensif à cause des modules de S1 qui débordent sur le S2. Dans l'ensemble l'année s'est plutôt bien déroulée mais la période décembre/janvier a été très dure pour certains. Au final tout le monde est heureux de ce master.

- « Théorie algorithmique des nombres pour la cryptographie »
  RV : L'enseignant de la partie bases de Groebner a une énergie incroyable, cours très bien, DS relativement apprécié mais trop court pour des questions qui prennent un peu de temps (calculs sur les bases de Groebner). Ce serait bien d'avoir une correction des TD et plus généralement plus de traces écrites. L'autre enseignant était plus timide et moins facile à

comprendre mais cours et DM très bien et intéressant, bien progressif. Matière globalement très appréciée.
DB : C'était une première pour l'enseignant de la partie courbes elliptiques et il a particulièrement apprécié l'expérience. Il continue cette année.

- « Codes correcteurs en cryptographie»
  RV : cours très bien structuré et apprécié, TD/TP intéressants. DM final pas très crypto mais apprécié quand même. Enseignante un peu déconcertante, parfois assez proche des étudiants et parfois assez dure (exemple du premier TP donné en avance et très facile, la plupart des étudiants ne sont donc pas venus à la séance en pensant qu'elle s'adressait plutôt aux étudiants de maths fondas et l'enseignante était très remontée).
  SD: étonnant que çà retombe sur les rares étudiants qui sont venus. Ceci dit c'est particulièrement désagréable quand on passe du temps à préparer une séance et que les étudiants ne viennent pas. Non dit lors de la réunion mais important : ce cours est un cours du master de cryptographie, les étudiants de maths fondas y ont accès mais ne sont pas le public cible, il n'y a donc pas de séance ou d'éléments du cours pensés pour eux.
- « Cryptographie quantique »
  RV : pas beaucoup de crypto, cours le plus apprécié du semestre et peut-être même du master, l'enseignant se donnait à fond et c'était génial. Début un peu lent pour donner les bases physiques et pas eu le temps de finir l'algorithme de Shor.
  SD : c'est normal qu'il y ait peu de cryptographie quantique, ce cours est mal nommé, il devrait s'intituler « algorithmique quantique en cryptographie » par exemple. L'enseignant s'est effectivement beaucoup investi dans la préparation de ce cours assez atypique et s'est très bien que le retour soit si positif.

<u>Bilan des stages de M2</u>

RV : plutôt des recommandations pour les prochaines promos que des retours sur les stages :

- faire attention au matériel disponible et à l'encadrement. Certains étudiants ont en effet rencontré quelques soucis avec l'impossibilité d'accéder à des distributions Linux ou les RH et les aspects administratifs,
- c'est bien de s'ouvrir vers d'autres domaines que la crypto, il y a plein de choses intéressantes à faire autour de la crypto, en cybersécurité et même au-delà (robotique par exemple cette année),
- identifier rapidement quelles matières sont les plus intéressantes et solliciter les entreprises du domaine via des candidatures spontanées. C'est plus facile de rester dans l'entreprise du stage si on vise dès le début un sujet sur lequel on est motivé,
- c'est bien de recevoir plein d'annonces d'offres de stages et d'avoir du choix.

AP : y a t'il eu beaucoup de candidatures spontanées ?
MV : non, mais les annonces ne permettent pas forcément de viser un sujet spécifique.
SD : encore une fois, les retours des entreprises sur les stages sont très positifs. C'était une grosse promo cette année et quelques étudiants ont difficilement trouvé un stage. Il y avait 26 étudiants inscrits. 23 ont validé l'année, 1 a changé d'orientation, 1 redouble et 1 a trouvé un emploi après son stage sans avoir validé le M2. La moitié continue sur le lieu de stage soit en CDI soit en thèse (c'est plus que d'habitude). En terme de sujets, on note cette année une très forte prévalence de la cryptographie post-quantique avec la moitié des stages sur ce sujet (pas étonnant du tout), mais aussi plusieurs stages thématiquement assez éloignés de la formation et qui se sont malgré tout très bien déroulés. Ca montre à la fois que les étudiants sont capables de s'ouvrir et que les entreprises ne s'intéressent pas qu'aux compétences déjà acquises.
MG : le but c'est aussi d'avoir un diplôme générique et de pouvoir s'adapter ensuite au cours de sa vie professionnelle.

Point sur les candidatures

SD : nous avons reçu cette année 125 candidatures en M1, ce qui est similaire à l'an dernier pour 20 places ouvertes. La promotion de cette année comporte 21 étudiants dont 7 femmes. Cela correspond à la proportion de femmes des années précédentes et il semble donc que la baisse enregistrée l'an dernier soit plutôt accidentelle que conjoncturelle.
Les conséquences pratiques de la mise en place de la plateforme monmaster relevées l'an dernier semblent se confirmer

- Pas plus de candidatures.
- Moins de réponses positives (Le 70eme classé a été pris à l'issu de la procédure cette année comme l'an dernier alors qu'on tournait autour de la 50eme place auparavant).
- Moins de désistement de dernière minute (effectif stable depuis fin juin/début juillet) en dehors des étudiants n'ayant pas validé leur L3.

Par contre, on ne note pas cette année une prévalence inhabituelle de candidats du périmètre Bretagne/pays de la Loire comme c'était le cas l'an dernier.

MG : il y a beaucoup plus de candidatures en master cyber (plus de 900). C'est peut-être du au fait que monmaster rend visible des formations qui ne l'étaient pas avant alors que le master crypto est déjà bien visible.

SD : en M2, il y avait 10 candidatures qui n'avaient pas fait le M1 crypto à Rennes et aucune admission car les prérequis sont importants et donc difficiles à rattraper. Il y a finalement 22 étudiants inscrits et aucun en parcours recherche.

Point sur la rentrée

SD : suite aux problèmes de mise en place de l'emploi du temps l'an dernier, le choix des options de M2 a été un peu plus contraint (possibilité pour des UE peu choisies les années passées de se chevaucher dans l'emploi du temps).
AP : ca a quand même affecté 2 étudiants qui voulaient suivre 2 cours qui se télescopent dans l'emploi du temps.
SD : il y a par contre eu pas mal de difficultés pour trouver des intervenants pour tous les cours, en particulier d'informatique. L'option AHP n'a par exemple pas pu ouvrir.

DB : l'emploi du temps du S2 en M1 est loin d'être idéal. Par exemple, le vendredi il y a ACGA à 8h et COCO à 16h15 et c'est tout.
SD : il faut arranger çà. Ceci dit les cours qui ne sont pas encore placés vont boucher certains trous.

MG : les mises à niveau en M1 sont très utiles mais ont été compliqués à mettre en place. L'ISTIC n'est pas motivé pour les prendre en charge et il est donc possible que l'UFR maths doive le faire.
AP : pas mal d'échanges entre les M1 et les M2 (aide pour l'installation des machines, avis sur les choix d'option, organisation de rencontres). Il n'y avait pas eu de tels contacts l'an dernier et c'est positif, c'est dommage qu'il n'y ait pas de BDE crypto alors qu'il y en a un à l'ISTIC.
SD : c'est même une excellente chose, ce serait bien que ça se pérennise. En ce qui concerne le BDE, ce n'est pas un BDE ISTIC, c'est un BDE cyberschool qui est censé regrouper les 2 promos.
AP : pas ou très peu d'interactions avec les cyber. Comme le BDE a déjà un an, ils se connaissent tous bien et ce n'est pas évident de rattraper le wagon. Il y a des cours en commun, mais seulement les CM et c'est pas l'endroit idéal pour échanger.

Concernant la relecture des CV et des lettres de motivation, le SOIE et la cyberschool peuvent donner un avis qui sera plutôt orienté vers les aspects RH. Pour les aspects plus techniques, il vaut mieux s'adresser à l'équipe pédagogique (en gardant en tête que notre expérience est assez limitée).