Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 14 février 2020

Présents: Romane Arvier (M1), Delphine Boucher, Mathieu Cima (M2), Sylvain Duquesne, Pierre Loidreau
Excusés : Christophe Ritzenthaler, Elisa Lorenzo Garcia
Absent : Patrick Derbez

Bilan du premier semestre de M1

RA : Globalement, tout va bien. Juste des petits soucis module par module à reporter

- **« Algorithmique de base »**
  RA : emploi du temps pas adapté : 6h tous les lundi, trop concentré. Au niveau du système de notation, ce n'était pas clair comment était attribué le point de TD (dépend trop de la difficulté de l'exercice sur lequel on passe) ou de TP (basé sur la présence alors que certains ont compris qu'il suffisait rendre un compte rendu).
  MC : il y avait déjà au moins 4h dans la même journée
  SD : Clairement pas normal pour l'emploi du temps. On sera attentifs l'an prochain.

  Présence de certains étudiants MF, qui venaient aux TP.

- **« Algèbre de base »**
  RA : Dur pour certains. C'est bien d'avoir un prof de TD spécifique.

- **« Programmation scientifique 1 »**
  RA : pas retours négatifs.

- **« Probabilités pour la théorie de l'information»**
  RA : Tout le monde a apprécié, rien à redire.

- **« Architecture, Système et Réseaux »**
  RA : Système de notation étrange (Quiz sur moodle bizarre car on peut le refaire autant de fois qu'on veut, TP noté sur seulement 5 questions). Contenu du cours OK mais commencé très tard.
  SD : Bizarre pour les quiz, pas gagné que le prof s'en soit rendu compte.
  MC : Pour les TP c'était comme çà dès l'an dernier. Par contre les Quiz en GPU ne pouvaient être faits qu'une seule fois.

- **« Anglais »**
  RA: Niveau très hétérogène donc difficile à gérer comme groupe d'autant que le groupe est petit (à cause des validations d'acquis). Ce serait mieux un groupe de niveau avec les CSM. Thématiques pas ou peu en lien avec la formation donc moins motivant. Beaucoup de travail oral.
  MC : L'an dernier, groupe mélangé avec les CSM.
  SD : C'est normal que ce ne soit pas en lien avec les sciences. L'objectif c'est de savoir communiquer (pour un entretien par exemple). La science ça vient tout seul ensuite et c'est pas le plus difficile.

- **« Histoire des maths »**
  RA : Très partagé. Certains aiment bien et d'autres pas du tout, n'en voient pas l'utilité ou l'interet. Pas de notes à cause des mouvements sociaux en cours.

MC : c'était pareil l'an dernier
SD/PL : La question revient effectivement régulièrement mais ça change, ça ouvre un peu culturellement. Et ca ne compte pas beaucoup à la fin.

- **« Semaine Profil »**
  RA : Pas parlé avec le reste de la promo. Certains ont fait plus d'ateliers que prévu et ils étaient bien (CV, lettres de motivation, entretiens). Pas de trop de soucis pour s'inscrire. Seul hic, il fallait s'inscrire pour le forum et les inscriptions étaient fermées.
  MC : C'était quand même possible s'y aller.

Bilan du premier semestre de M2

MC : Plein de bonnes matières, c'est très bien, il y en avait pour tout le monde mais plusieurs où on a l'impression de pas être à notre place : modules pas pensé pour cette formation.
Beaucoup de travail personnel demandé. Surpris de certaines notes par rapport à l'impression laissée par l'évaluation (dans un sens ou dans l'autre).
Grosse période très chargée (novembre/décembre) avec les recherche de stage .
Impression d'avoir appris plein de choses et prêts à être cryptologue

Bilan plus négatif pour le parcours recherche : impression d'être oubliés, en équilibre entre les 2 formations (crypto et maths fondas) et nombreuses matières pas du tout orientées cryptographie. Pourquoi pas commencer dès le M1. Finalement pas une très bonne expérience alors qu'il y avait du potentiel.
SD : On essaye d'avertir les étudiants que c'est un parcours difficile et exigeant. Le soucis c'est que ca dépend des cours proposés en M2 de maths fondas et que cette année, ils sont très éloignés de la crypto. Il faut être encore plus stricts sur les personnes acceptées et plus les informer.

- **« Courbes algébriques »**
  MC : Première partie très théorique avec un bon contenu mais pas assez de bases en géométrie projective : la prof a fait un effort d'introduction, mais pas évident. Examen très compliqué mais notes correctes : impression que la notation a été adaptée.
  SD : L'enseignante était effectivement satisfaite de ce qui a été fait à l'examen.
  MC : Contenu très intéressant sur la seconde partie. Ca aurait été bien d'avoir un peu plus sur les aspects appliqués (détails d'implémentations). Impression d'examen facile mais finalement raté. Les TD étaient très, TP bien sur le contenu aussi mais réticences sur magma. OK d'apprendre un nouveau logiciel mais pas possible de s'en servir chez soi (limite de temps de calcul de de la version gratuite trop basse). Beaucoup de réimplantation plutôt que d'utiliser l'existant. Pas besoin d'utiliser magma pour une fenêtre glissante. Notation bizarre du DM et trop long.
  SD : Moi aussi je pensais que l'examen était simple et j'ai été déçu par les copies. Dommage qu'il y ait eu plusieurs questions un peu similaires car ca amplifie les erreurs.
  DB: pas beaucoup de crédits par rapport au contenu
  SD : C'est vrai mais il fallait libérer des crédits (et des heures) pour les codes correcteurs.

- **« Programmation 1 (Java) »**
  MC : Gros point fort, les TP qui sont très ciblés crypto et très professionnalisant (réutilisé dans certains entretiens). Maîtrisent finalement bien java même si ca demande beaucoup d'investissement. Il faudrait inverser le premier (très dur) et le dernier TP (facile). Par contre, les CM c'est beaucoup de temps de perdu en particulier toute la première partie du cours c'est de l'algorithmique de base. Concept de classe long à venir et basé sur des classes développées par l'enseignant. Manque une partie de cours sur les fondements de java. Trop d'ECTS. Il ne faudrait garder que les TP. Examen pas terrible car sur papier.

SD : Même retour l'an dernier sur le premier et le dernier TP → à revoir. Le contenu du cours pourra être revu à l'occasion de la mise en place de l'EUR.

- **« C++, les bases »**
  MC : Très bien, très clair. Vraiment compris ce qu'est le C++. Examen difficile en particulier si on a raté la première question. Beaucoup regrettent de ne pas avoir été plus loin ou la possibilité de suivre la seconde partie du cours. Pourquoi pas le rendre obligatoire. Et y rajouter les TP de Java.
  SD : la 2eme partie est inintéressante pour les crypto. Elle se concentre sur l'étude de bibliothèques spécifiques au calcul scientifique. Est ce que ce serait pas trop compliqué de ne faire que les TP de Java sans connaître ce langage.
  MC : Pas de soucis si on a fait les devoirs de vacances.

- **« GPU »**
  MC : pas de soucis avec l'anglais. Contenu de la première partie très intéressant. Essai pédagogique du format de cours (mélange CM/TP par blocs de 15mn) pas concluant (CM trop rapide et TP trop passif ou pas le temps de le faire). Examen de programmation sur papier également assez exigeant. Projet final (de CSM) de parallélisation. Mélange des groupes avec les CSM trop peu nombreux (1 pour 3). Difficultés sur les maths et sur des choses implicites. Ce serait mieux d'avoir un projet crypto. Ou en tous cas de mettre moins de trucs spécifiques. La note finale dépendait trop du sérieux du CSM du groupe. Quelques quiz au début surtout pour voir où on en est qui comptent peu.
  SD : Assez étonnant, d'habitude il y a plus d'étudiants de CSM que de crypto dans ce cours. Réorienter les sujets de projets si cette tendance se confirme.
  DB: L'enseignante est spécialiste du domaine d'où des sujets orientés CSM
  MC : 2eme partie sur le GPU qui compte trop dans la note finale par rapport à son poids dans le module. Examen bizarre et déstabilisant (très général). Enseignant compétent mais le déroulé du cours manque un peu d'organisation.

- **« Sécurité des données pour la propriété intellectuelle et la vie privée »**
  MC : Contenu très intéressant mais MCC un peu floues. Projet très intéressant mais cahier des charges et barème peu clair. examen écrit assez inégale**.** Séances de TP pas vraiment utiles indépendants du cours mais intéressant. Plutôt adaptés à Supelec au niveau info et ça mériterait d'être un peu plus guidé pour les étudiants de crypto. Manque des TD.
  SD : Même retour l'an dernier pour les TD. C'est classique des cours de M2 qu'il n'y ait pas de TD, c'est un module avec le parcours recherche en informatique

- « **Résolution de challenges de sécurité** »
  MC : Beaucoup d'appréhension suite aux retours de l'an dernier mais visiblement beaucoup d'améliorations (pas que du rootme pour l'évaluation par exemple). Bilan positif.
  SD : C'est une bonne chose que ce qui est remonté dans cette réunion se traduise par des améliorations effectives de la formation.

- **« Protocoles de sécurité »**
  MC : Bilan très paradoxal. Semble indispensable mais impression que c'est mal abordé, trop tourné vers la connaissance des langages de preuve formelle. Difficulté à voir l'intérêt ou l'utilité pour la suite. Notation dure de l'examen.

- **« Anglais »**
  MC : Contenu très bien même si c'est pas orienté crypto. Mais beaucoup de travail personnel à des moments un peu tendus pour le reste. Groupes de niveau plutot positifs.

- **« Semaine Profil »**
  MC : Bilan très mitigé. Ateliers d'entretiens d'embauche, CV, lettre de motivation étaient très bien et utile (dommage qu'il y ait eu des annulations de dernière minute). D'un autre coté, certains y voient une perte de temps dans un emploi du temps très chargé (projets en particulier). Certains ateliers ont étonné voire plus (sophrologie, homéopathie, ...). Forum intéressant mais trop peu de crypto.
  Le forum cyber de Supelec était beaucoup plus intéressant et bien plus orienté crypto. Une personne y a trouvé son stage.
  SD : C'est normal car le forum de Rennes 1 s'adresse à tous alors que celui de Supelec est spécifique Cyber. Il faudra faire plus d'information dessus à l'avenir. C'est très positif que les ateliers CV/entretien aient rempli leur rôle.
  PL : confirme que savoir rédiger un CV est très important.

- **« SIMP »**
  MC : très intéressant et utile voire le plus utile de la formation. Pas de soucis avec l'anglais mais impression que l'enseignant en aurait dit plus en francais. TP très bien aussi mais pas adapté aux PC de la salle info et difficile a installer sur les portables. Cahier des charges pas extra clair mais. Examen OK et pertinent (recherche de faille) mais dommage qu'il n'était pas possible de les trouver toutes dans le temps imparti.
  SD : Dommage qu'il y ait ces freins. A terme, il devrait y avoir une salle info dédiée qu'on pourra plus facilement adapter aux besoins des enseignements.
  MC : Par rapport aux étudiants de Cybersécurité, les étudiants sont avantagés sur certaines parties et désavantagés sur d'autres

- **« Codes correcteurs en cryptographie »**
  MC :1ere partie très bien et bien construite, continuité avec l'an dernier (mais du coup problématique pour les nouveaux). Des TD auraient pu etre bien. Module pas simple mais accessible, il faut fournir du travail. Contenu du DM très bien, implémentation pas facile mais ca aurait été bien d'avoir un cahier des charges un peu plus précis sur ce qui était attendu.
  DB: Dommage qu'il y avait quelques erreurs dans l'énoncé…
  MC : Examen bien adapté et oral de rattrapage (non obligatoire) apprécié. 2eme partie du cours avec un bon contenu très orienté crypto mais examen beaucoup trop long.

- **« Cours du Master recherche»**
  MC : Le module « Théorie de l'intersection » était particulièrement problématique et avait trop d'importance pour une matière non crypto. Trop de prérequis non acquis en M1 (catégories). Enseignant pas très coopératif (renvoie vers Bourbaki pour apprendre les catégories) et problèmes de communication (certaines informations n'ont été transmises qu'aux maths fondas). Impression de jugement de valeur entre les maths fondas et les crypto. Examen trop compliqué et exigeant et pas d'oral de rattrapage alors qu'un était promis. Bref pas du tout adapté à des étudiants de crypto et ça plombe la moyenne à cause du coefficient.
  SD : C'est étonnant car les catégories ne sont pas non plus au programme du M1 maths fondas. Pour le reste, il faudra vraiment faire beaucoup plus attention l'an prochain sur les choix de cours mais de toutes façons, cette année, il n'y avait rien de proche de la crypto.
  PL : Pourquoi pas ouvrir vers les autres parcours, en particulier le parcours de stats ou de proba, plus accessible et plus utile.
  DB: Attention, ils auront aussi des lacunes au départ.
- **MC** : En ce qui concerne le séminaire, heureusement qu'il était là. Très interessant. En particulier la découverte de la recherche et les interactions avec les enseignants chercheurs

<u>Point sur les stages</u>
SD : 1 étudiant n'a pas encore trouvé de stage à ce jour mais il a plusieurs pistes et 1 ne vient plus en

cours.
MC : pas si difficile de trouver un stage une fois qu'on ose candidater (l'entretien est presque une formalité) car on gagne en confiance. Certains ont même eu le choix.

Mise en place de l'école universitaire de recherche Cyberschool

Ecole de type graduate school pilotée par Pierre-Alain Fouque (ISTIC) et David Pichardie (ENS Rennes) avec un budget d'environ 5 millions d'euros pour 10 ans

Objectifs

- Doubler le nombre d'étudiants formés en cybesécurité à Rennes en 10 ans : on passerait de 100 à 200 étudiants de master par an et de 30 à 60 doctorants.
- 6 thématiques principales (logiciel, matériel, méthodes formelles, IA, droit et cryptographie) mutualisé entre tous les partenaires (IMT, ENS, UR1, UR2, Supelec, INSA)
- Approche interdisciplinaire via des majeures et des mineures sur ces 6 thématiques.
- Réorienter la formation vers la recherche via des stages de recherche en labo systématiques.
- Augmenter les débouchés des doctorants vers l'industrie.

Moyens/actions

- Aménagement du batiment 13 avec des salles dédiées.
- Des moyens humains (ingénieur pédagogique, manager d'études, international).
- Bourses de master pour attirer des étudiants en particulier étrangers.
- Bourses de thèses.
- Écoles d'été
- Programme de mobilité au sein d'un réseau d'universités étrangères

Ouverture à la rentrée 2020 pour le M1

- On commence par se coordonner au niveau UR1 avant d'étendre aux autres établissements.
- Cours en anglais si il y a un étudiant dans la salle qui ne parle pas français.
- 3 conséquences sur la formation envisagées
    - Remplacement de PSC1 par un module de programmation bas niveau (C+assembleur) mutualisé avec la cybersécurité et concentré en début de semestre.
    - Création d'un cours de machine learning mutualisé également et assuré par Valérie Monbet à la place d'ACGA. Cours d'initiation sans prérequis.
    - Remplacement du cours "architecture/système/réseaux" par un cours plus spécifique réseaux mais avec une dimension sécurité qui donnera une meilleure pour SRES.

A terme l'offre devrait s'étoffer pour les options de M2.

Questions diverses

- Création d'un groupe LinkedIn pour relancer le réseaux des anciens étudiants qui commencent à être nombreux.
- Il faut informer les étudiants des journées de mise en oeuvre de la crypto post-quantique en mars.
- Problèmes de fausse manipulation sur les emplois du temps du M1 : DB s'est fait piquer des créneaux