Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 8 février 2017

Présents: Angèle Bossuat (M2), Patrick Derbez, Sylvain Duquesne, Pierre Loidreau, Sarah Paardekooper (M1)

Excusés : Delphine Boucher, Xavier Caruso, Christophe Ritzenthaler.

Invité : Shane Byramjee (stagiaire de 3ème)

Composition du comité

Patrick Derbez remplace Pierre Alain Fouque comme représentant de l'ISTIC dans le comité

Bilan des cours de M2

L'année a souvent été jugée globalement décevante à cause de l'impression de saupoudrage : plein de sujets ont été abordés sans aller au fond des choses (TANC, SRI). Il est clair qu'on a pas le temps de voir tout mais qu'il est quand même important que ces notions soient abordées pour avoir une base pour les creuser éventuellement par la suite si nécessaire.
Les étudiants auraient aimé avoir plus d'information sur les options en début d'année. Un effort sera fait sur ce point l'an prochain.

- **« Courbes algébriques »**
  Cours intéressant et bien. En plus bien complété par « Cryptographie avancée ». Les étudiants ont toutefois été étonnés de faire un QCM en CC sur des sujets qui demandent à priori des justifications,
  Ce cours était fait en anglais cette année à titre expérimental car l'université souhaite imposer un cours en anglais chaque année dans toutes les formations. Le principe est bien mais cela pose problème à environ 70 % des étudiants et plus particulièrement aux étudiants étrangers qui n'ont jamais fait d'anglais avant. Ça tombe mal de le faire sur un cours difficile et sur un sujet nouveau. Le cours devrait donc repasser en français l'an prochain (sauf contrainte officielle de l'université)
- **« Théorie des nombres »,**
  Le cours est bien mais il y a un gros problème d'organisation : l'enseignant utilise des transparents et les étudiants passent leur temps à les recopier plutôt qu'à comprendre le cours. Il suffirait de distribuer une copie papier des transparents pour régler ce problème. Ce sera suggéré à l'enseignant. Il y a également eu une incompréhension sur les TP mais cela ne se reproduira plus l'an prochain en raison du changement d'organisation du master (voir plus loin). Il y a également eu un problème de décalage entre les méthodes utilisées par l'intervenant de TD et celles vues en cours. Ce sera remonté aux enseignants.
- **« Cryptographie avancée »**
  La partie asymétrique est très bien mais peut-être un peu trop théorique. Comme chaque année le choix de magma étonne les étudiants. Ce choix est cependant fait en connaissance de cause. Magma est un logiciel très utilisé en crypto et fait certaines choses que sage ne sait pas bien faire. Mais surtout changer de langage entraîne les étudiants à s'adapter à un nouveau langage de programmation. C'est donc normal (et voulu) que les étudiants se retrouvent mal à l'aise face à un nouveau langage qui n'apporte (c'est vrai) rien de plus que sage pour le contenu de ce cours. La capacité d'adaptation des diplômés de ce master est leur meilleur atout (et reconnu comme tel par industriels du secteur).
  Concernant la partie symétrique, c'est bien de savoir enfin comment on attaque l'AES (6 tours). C'est juste dommage que l'examen n'ai pas trop de rapport avec le cours (amplifié par le temps trop long entre la fin du cours et l'examen). Ce serait bien aussi d'avoir des slides ou un poly et

ça aurait été bien d'avoir un DM. Patrick Derbez prend bien note de ces retours.

- **« Programmation 1 (Java) »**
  Les étudiants sont très content d'avoir des TP adaptés pour les crypto. Dommage que ce soit pas pareil pour les TD car les L3 sont insupportables. Et du coup ça avance beaucoup moins vite et moins bien.
- **« Sécurité des Réseaux Informatiques »**
  C'est un module difficile et il y a trop d'intervenants. L'ISTIC est au courant de ce problème qui n'est pas nouveau mais personne ne veut vraiment s'investir dedans. Ils ne savent pas vraiment comment ça va se continuer l'an prochain. Les étudiants ont aussi trop de lacunes en réseau. Un autre problème est qu'il y a trop de différence avec les SSI (dans les 2 sens). Idéalement, il faudrait forcer les étudiants à faire des binômes SSI/crypto et ça permettrait en plus de se mélanger et d'apprendre à travailler avec des personnes ayant un bagage différent.
- **« Réussir son insertion professionnelle »**
  Les cours ont commencé trop tard (mi-octobre). Certains avaient déjà eu des entretiens. Les simulations c'était bien. Par contre les heures de cours avaient un contenu trop peu dense. Il doit être possible de proposer le même contenu en 4h de cours ce qui permettrait de faire 4h d'entretien (d'autant que la plupart du contenu est sur Triptik)
- **« Anglais »**
  Trop de cours pour un si petit module et ça prend trop de temps par rapport au reste. Et surtout sans avoir l'impression de progresser. Quelque soit l'orientation future, l'anglais reste fondamental et indispensable même si çà paraît moins motivant que les autres cours. Les étudiants préféreraient avoir autre chose que des maths ou des sciences comme sujets d'étude. Ce sera remonté aux intervenants.
- **« Cryptographie Quantique »**
  Très intéressant et bien
- **« C++, les bases »**
  Long mais intéressant, Enseignant très disponible
- « **Résolution de challenges de sécurité** »
  C'est un module de second semestre, mais Patrick Derbez préfère profiter de sa présence pour avoir des retours.
  Module un peu brouillon en particulier sur ce qui est attendu du contenu des rapports. Dommage de pas avoir de correction des premiers challenges (mais les SSI n'en veulent pas). Ce serait bien aussi de faire un petit bilan sur les compétences manquantes en début de cours pour faire un cours de rattrapage. Il faudrait plus cadrer les challenges visés. Il y a peut-être un peu trop d'autonomie. Le problème c'est que les SSI demandent le contraire. Il faudrait donc différencier, au moins sur la partie évaluée. Les étudiants ont particulièrement apprécié qu'un intervenant extérieur vienne expliquer ce que c'est que résoudre un challenge. Ce serait bien que ça commence plus tôt dans l'année pour avoir plus de temps pour résoudre les challenges. C'est prévu pour l'an prochain,

Point sur les stages

Presque tous les étudiants ont trouvé un stage même si ça a été un peu difficile pour les derniers. En SSI c'est mieux que l'an dernier aussi. Tout s'est débloqué sur le mois de janvier. Un point particulièrement dommageable est qu'Amossys, pourtant parrain de la formation, n'a pas répondu aux candidatures.

Bilan du premier semestre de M1

Sarah Paardekooper, représentante des M1, n'a été prévenue que tardivement de la tenue de la réunion et avait donc moins de commentaires à faire qu'Angèle Bossuat.

- **« Algorithmique de base »**
  Pas de remarques particulière. Le module et son niveau ont été appréciés.
- **« Algèbre de base »**
  Module toujours difficile. Les étudiants ont particulièrement peu apprécié d'avoir un cours pendant la semaine de révision. Suite aux retours de l'an dernier, le coefficient de ce module pour le calcul de la moyenne a été ramené à 6 (au lieu de 9).
- **« Programmation scientifique 1 »**
  Les étudiants n'ont pas as eu les notes de CC et de projet. Ce module est trop orienté vers les étudiants de CSA.
- **« Probabilités pour la théorie de l'information»**
  Les énoncés des contrôles étaient un peu long mais l'enseignant en a tenu compte dans la notation. Le contenu était OK
- **« Architecture, Système et Réseaux »**
  Rien à dire. Les retours de l'an dernier (pas assez de TD) ont été pris en compte cette année.
- **« Réussir son insertion professionnelle »**
  Le cours était bien mais ce serait bien d'avoir un contact. Les étudiants ont envoyé leur modèle de CV sur une adresse visiblement non lue par l'intervenante et n'ont par conséquent pas eu de retour dessus.
- **« Anglais »**
  Trop hétérogène car pas de groupe de niveaux et du coup seuls les meilleurs étudiants participent. Ce serait vraiment mieux avec des groupes de niveau même si le risque est une baisse de participation du fait de se retrouver avec des étudiants moins familiers.

Prochaine habilitation (2017-2022)

La maquette de l'habilitation 2017-2022 est présentée au comité (ci-dessous avec les nouveautés en rouge). Les principaux changements sont

- THNO passe en M1S2
- ACGA passe en M2S2 et est réduit de moitié (la moitié AC)
- Certains volumes horaires ont été augmentés
- ALGB passe à 8 ECTS et ASR à 4 en M1
- Nouveaux cours sur les réseaux en M2
- Réduction du cours de cryptographie avancée aux courbes elliptiques (suppression de LLL, qui passe dans le cours sur les réseaux, des couplages et de la cryptanalyse symétrique) et passage de 6 à 3 ECTS
- Disparition de « Environnement économique et juridique de l'entreprise ». Il y aura toutefois une ou 2 interventions sur le sujet avec la même intervenante en commun avec les SSI
- Cryptographie quantique devient obligatoire en M2
- Nouveaux choix d'options

Une discussion s'engage sur la disparition de la cryptanalyse symétrique suite à une incompréhension entre les responsables des master crypto et SSI. C'est indispensable que les étudiants aient des notions dans ce domaine (attaques différentielles et linéaires au moins). Il y en avait déjà trop peu (10h au total). Il est convenu que cette partie sera intégrée au cours de S10 « Théorie Algorithmique des Nombres pour la Cryptographie » qui a justement vu son volume horaire augmenter de 10h (initialement pour faire les couplages).

Remarque : La formation a été labellisée par l'ANSSI
https://www.ssi.gouv.fr/particulier/formations/secnumedu/formations-labellisees-secnumedu/

Master Mathématiques de l'information, Cryptographie 2017-2022

M1

Semestre 7 (30 ECTS, 126 CM / 112 TD / 54 TP)
• Algèbre de base (**8**, 36/36/6) • Algorithmique de base (6, 24/24/12) • Probabilités pour la théorie de l'information (6, **30/30**/0) • Programmation Scientifique 1 (6, 18/12/18) • Architecture, systèmes, réseaux (**4, 18/0/18**) • Réussir son insertion professionnelle (0, 10)
Semestre 8 (30 ECTS, 88 CM / 102 TD / 34 TP)
• **Théorie des nombres (6, 24/24/6)** • Codes correcteurs (6, 24/16/12) • Cryptographie (6, 24/16/16) • Projet tutoré (6, 0) • Complexité (3, **16/16/0**) • Anglais (3, 30)

présentiel étudiant : 516h

M2

Voie Classique	Voie Recherche
Semestre 9 (30 ECTS)	
• Courbes algébriques (3, 12/12/0) • **Courbes elliptiques pour la cryptographie (3, 12/8/8)** • **Réseaux euclidiens en cryptographie (3, 20/16/2)** • Cryptographie quantique (3, **16/16**/0)	
Programmation 1 (6, 0/32/22) Sécurité des réseaux informatiques (3, 16/4/12) 3 UE à choisir (3x3, variable) Réussir son insertion professionnelle (0, 10)	Algèbre-Géométrie 1, 2, 3 ou 4 (6, 24/24/0) Algèbre-Géométrie 1, 2, 3 ou 4 (6, 24/24/0) Séminaire (6)
Semestre 10 (30 ECTS)	
• Théorie algorithmique des nombres pour la cryptographie (3, **16/12/6**) • Anglais (3, 30) • Stage (18)	
Canaux auxiliaires (3, **16/16/0**) **Algèbre commutative (3, 12/12/6)**	Algèbre-Géométrie 5, 6, 7 ou 8 (6, 24/24/0)

UE à choix

- **protocoles de sécurité (20/0/0)**
- C++, les bases (12/0/12)
- Programmation parallèle et sur GPU (12/0/16)
- **Sécurité des données pour la propriété intellectuelle et la vie privée (20/0/0)**
- **Sécurité système (16/0/16)**
- **Résolution de challenges de sécurité (16/0/16)**

présentiel étudiant classique : 404 à 428h
présentiel étudiant recherche : 330h