Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 15 mars 2013

Présents:

Bilan des cours de M2

theorie des nombres avancée
corps finis : pb sur les corps de fonction et les corps p-adiques.
Le ALGB de M1 semble OK, plus au niveau manipulation
devoir maison. Contenu des cours suffisant
voir les livres et les prerequis
manque surtout de la pratique
AGM trop dur
emploi du temps pas assez étalé

- « Courbes algébriques »
  pas assez d'heures parce que ca va trop vite ou plus de TD.
  Rediscuter le contenu

- « Cryptographie avancée »
  emploi du temps.
- « ASR »
  intervenant pas plu. Etude des produits CISCO. Que du reseau et pour specialiste utile pour des admin reseau. Pas compris grand chose.
- « Systèmes d'exploitation, Réseaux informatiques, Sécurité »
  Intervenant (pas le même que d'habitude qui était en délégation cette année) pas top, plein de fautes, pas au point. Partie sécurité par Bekalli bien.
- Java
  TP orienté crypto c'est bien
  plus de C++ et moins de Java, problème de personne avec l'intervenant . Pas assez orienté objet (une seule classe).
  Aucun retour en M1.
- « C++ »
  vraiment bien, arreté un peu tôt. Ils auraient aimé aller plus loin
- « crypto Q »
  crypto juste dans le dernier cours sinon c'est que des espaces de Hilbert, il faudrait que ca vienne un peu plus tôt. Pas de q-bit et il manque la correspondance avec la physique quantique.
- SRI
  un peu fourre tout (plein d'intervenants). Profs etonnés de voir des crypto. Manques en reseau. Prevenir les intervenants. Surtout pour IPSEC/VPN mais pour d'autres groupes aussi.
- « Technique de recherche d'emploi »
  TB.
  Par grand chose en cryptographie au forum
- « Anglais »
  Groupe de niveau mais très mal faits. Ca depend des intervenants. toujours pas de prépa au CLES.
- « Protection de contenu »
  bien pour la culture générale a prendre en surnumeraire

- « Protection de la vie privée »
  tout ou rien suivant
- « Auth »
  beaucoup de deja vu (pas illogique). Idem en SSI ca va evoluer
- « Cryptographie quantique »
  Intéressant, prof très bien et il fait tout ce qu'il peut pour que tout le monde comprenne, beaucoup de rappels
- « programmation parallèle, GPU »
  bien, cours en anglais c'est bien.
- « IDS »
  TB tres interessant mais difficile
- « Carte à puce »
  bien, mais ce serait mieux d'avoir plus d'heures, surtout des TP, exam sympa (article)
- « Environnement économique et juridique de l'entreprise »
  génial à la surprise générale.

Globalement edt desordonné

Point sur les stages

il en manque encore 1. Visiblement certains stages ont été annulés (Orange, aucune réponse de la DGSE alors qu'ils proposaient beaucoup de stages qui auraient du diminuer la pression sur le marché)

D'un point de vue général, il manque un cours pour expliquer comment se tenir au courant en crypto, presse crypto.

Bilan du premier semestre de M1

- « Algorithmique de base »
  Assez difficile mais ca a plu. Peu de retour.
- « Algèbre de base »
  Plutot difficile mais peu de retours
- « Programmation scientifique 1 »
  trop axé modélisation et pas de crypto. Prevenir au début de l'année. Facon surprenante de noter les TP.
- « Proba»
  OK
  bien, pas mal de TP (en maple). Un peu déroutant. Difficultés sur les corps finis. Plus de temps sur les BCH serait appréciable,
- RIP
  OK mais général sur l'insertion et ne connait pas le millieu
- « Anglais »
  pas de groupe de niveau. Pas de problème d'hétérogénéité car l'enseignant (Nicolas André) gère bien

  Globalement TT à prendre en compte de facon plus respectueuse (bazar au debut ou à la fin du temps officiel)

Association des anciens étudiants

personne pour s'en occuper
recontacter la fondation

Survit difficilement car personne ne veut y consacrer du temps. Kelly Resche veut bien s'en occuper. Sont évoqués les points suivants

- Il faut un site (hébergé par l'université)
- Il faut maintenir une liste à jour des anciens élèves avec coordonnées et emploi
- Il ne faut pas hésiter à demander des financements au CEVU pour organiser des actions
- Ce serait bien d'avoir un mail de redirection d'anciens du type prenom.nom@crypto-rennes.org à défaut d'avoir prenom.nom@univ-rennes1.org que l'université ne veut pas mettre en place (mais il faut demander à la fondation rennes1)

Avenir du Master
L'université a mis le master en alerte du fait du trop faible flux d'étudiant et de la trop faible mutualisation. Se rajoutent à ça des problèmes d'ordre pédagogiques (Théorie des nombres en même temps que Algèbre de base, Programmation scientifique 1 pas bien adapté, pas de programmation objet, codes correcteurs avancés inutile) et d'ordre administratif (coût des interventions extérieures, trop faible implication de l'UFR, effectif officiel trop faible en crypto quantique)

Propositions d'aménagements

Accepter 15 étudiants en M2 chaque année

a) Baisser le niveau d'exigence à l'entrée en M2, en particulier en termes de prérequis quitte à les faire redoubler ensuite en leur demandant de suivre les cours de M1 à la place du stage
b) Créer un parcours recherche 100% mutualisé entre le master crypto et le master recherche en algèbre et géométrie
c) Double diplôme Karlsruhe (étudiants en Allemagne en pratique mais inscrits aussi à Rennes)
d) Pas de souci l'an prochain car le flux en M1 est en forte augmentation (21 au lieu de 13)
e) Ne même pas essayer d'avoir 15 étudiants en s'appuyant sur d'autres arguments « orchidée » (taux d'insertion excellent, liens avec les entreprises, taxe d'apprentissage, montée en puissance de la crypto à Rennes)

Déplacer Théorie des nombres en S3

Codes correcteurs avancés est déplacé en M1 pour fusionner avec le cours de codes et former un cours de 6 ECTS assuré par l'UFR. Il est placé en S2 afin d'être proposé également en M1 maths. Le contenu est réorienté vers les codes algébriques.

Java et C++ sont remplacés par PRG1, cours de programmation objet du L3 info avec possibilité de faire des TP spécifique crypto.

Couper Systèmes et réseaux en 2
3 crédits pour systèmes et réseaux généraux, 3 autres pour sécurité des réseaux.
Permet d'introduire l'architecture et les systèmes plus tôt dans la formation et d'équilibrer les 2 années en terme de ratio maths/info. Cela n'a pas été évoqué lors du comité mais la partie sécurité sera mutualisée avec le Master SSI.

Programmation scientifique est proposé seulement au choix pour les étudiants qui n'auraient pas fait de C avant dans leur formation et un cours d'introduction au C y sera inclus.

Cela donnerait l'organisation suivante

Semestre 1
Algèbre de base (9)
Algorithmique de base (6)
Cryptographie (6)
Programmation scientifique 1 ou Programmation 1 (6)
Systèmes et réseaux (3)

Semestre 2
Algèbre commutative et géométrie algébrique (6)
Codes correcteurs d'erreurs (6)
Probabilités pour la théorie de l'information (6)
Projet tutoré (6)
Complexité (3)
Anglais (3)

Semestre 3
Cryptographie avancée (6)
Théorie des nombres (6)
Programmation 1 (6) ou C++, les bases (3) et cryptographie quantique (3)
Courbes algébriques (première moitié de l'actuel Maths pour la crypto) (3)
Sécurité des réseaux informatiques (3)
Option (3)
Anglais (3)

Semestre 4
Cartes à puces (3)
Environnement économique et juridique de l'entreprise (3)
Théorie algorithmique des nombres pour la cryptographie (deuxième moitié de l'actuel Maths pour la crypto) (3)
Option (3)
Stage (18)

Notez que cette proposition est encore suspendue à un éventuel passage de théorie des nombres en S2 (le problème de l'articulation entre ALGB et THNO n'est pas spécifique au master crypto)