

## Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 17 juin 2011

Présents: Didier Alquié, Antoine Chambert-Loir, Sylvain Duquesne, Mohamed El Belghiti (M2), Marie Alice Lossois (M1).

### Bilan du second semestre de M1

- « Algèbre commutative et géométrie algébrique (AGCA) »  
**MAL** : OK
- « Logique, Théorie des modèles et Complexité (LTMC) »  
**MAL** : la partie logique ne sert à rien, la partie complexité est trop courte en particulier pas assez de TD pourtant y'avait des exos à la maison et un DM.  
**ACL** : pas assez d'heures donc presque que du cours, exercices trop durs. Partie automates OK, mais la partie machines de Turing et complexité c'est dur (surtout pour ceux qui n'ont pas fait fait ALBA).  
**Discussion** : des exercices et un DM ont été donnés en autonomie, mais il faudrait en rajouter des plus simples pour l'an prochain. AKS est fait en M2 par DA, ça libérera donc des heures pour prendre un peu plus de temps sur le reste l'an prochain. La partie logique disparaîtra à partir de 2012-2013. C'est dommage que les étudiants ne voient pas le lien entre les 2 parties du cours.
- « Théorie de l'information, codage et cryptographie (THIC) »  
**MAL** : OK mais ce serait bien de faire les TP en C  
**SD** : Le but des TP n'est pas d'apprendre le C, mais de manipuler les objets du cours et il y a plus d'outils avec Maple et les étudiants sont plus à l'aise. Il faudrait par contre envisager de passer à Sage.
- « Projet tutoré »  
**MAL** : OK. L'anglais c'est bien mais c'est dur pour ceux qui écoutent surtout avec 5 ou 6 soutenances dans la journée.
- « Anglais »  
**MAL** : OK
- Bilan global : 12 étudiants ont suivi le parcours, 1 a disparu, 5 sont reçus en première session et 3 ou 4 en seconde.

### Bilan du second semestre de M2

- « Cartes à puces »  
**MEB** : cours bien, ce serait bien qu'il y ait des TP. Mini projet TB  
**SD** : Ces cours ne comportent à priori pas de TP. Ceci dit, je ne l'ai pas évoqué pendant le comité mais il y en aura probablement dans la prochaine habilitation car ce cours sera mutualisé avec SSI.
- « Codes correcteurs »  
**MEB** : cours pas structuré, les étudiants n'ont pas appris grand chose et décrochent rapidement. Aide pour le projet appréciable car au départ c'était chaud.
- « Cryptographie quantique »  
**MEB** : pas de retour
- « Stages »  
Ça se passe bien d'après les rapports à mi-stage et les retours des encadrants. Pour l'instant, un étudiant fait une thèse DGA l'an prochain et un sera probablement embauché sur son lieu de stage. Il faut rappeler qu'il est plus que temps de se mettre à chercher très activement un emploi.

### Association des anciens étudiants

Il est fondamental et dans l'intérêt des étudiants de faire vivre l'association des anciens. En particulier au niveau de l'annuaire. Comme évoqué après la réunion avec Mohammed, ça peut se faire sous la forme d'un groupe facebook (mais à accès restreint) par exemple. Ce n'est pas la peine de faire quelque chose de compliqué mais il faut que ça reste à jour. D'autre part, une demande de subvention raisonnable au CEVU (1000-2000€), sera probablement acceptée. Ça permettra d'organiser plus facilement des rencontres entre anciens, quitte à avoir un ou 2 invités pour faire une conférence.

### Organisation 2001-2012

37 dossiers pour le M2 dont une majorité d'étrangers.

L'organisation du M2 sera un peu différente : C++ et MACR auront lieu plutôt en début de semestre et CRAV et PRAV plutôt en fin pour tenir compte des remarques de cette année.

Il est probable que les cours d'anglais se feront dans des groupes d'info plutôt que de maths pour régler le problème d'emploi du temps crée par protection de contenu.