Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 2 mars 2012

Présents: Didier Alquié, Sandrine Blazy, Vincent Breger (M2), Sylvain Duquesne, Pierre Loidreau, Kelly Resche (M1)

Bilan du premier semestre de M2

- « Mathématiques pour la cryptographie »
  VB : globalement satisfaisant même si comme les autres années il n'y a pas assez d'heures pour ce module.
  SD : il n'y a malheureusement pas de miracle surtout vu l'étendue de la géométrie algébrique à moins de supprimer les TD mais ce n'est pas une bonne solution.
  Cette année, le cours a été décalé par rapport à celui de crypto avancée. C'est mieux mais idéalement il faudrait le faire complètement avant.
- « Cryptographie avancée »
  VB : pas grand chose à dire,
  SD : L'an dernier, les étudiants avaient eues quelques difficultés, notamment sur les couplages. Cette année, on a pris plus de temps pour les faire.
- « Programmation pour la cryptographie »
  VB : TB, TP interessants, que des retours positifs.
  SD : Le tutoriel de Java et le travail demandé pendant les vacances en Java (DSA) semble avoir porté ses fruits. A continuer donc.
- « Systèmes d'exploitation, Réseaux informatiques, Sécurité »
  VB : TB pas bcp de questions des etudiants. Pas assez d'aspects securité en TP. Rapports de TP difficile jusqu'à ce que l'encadrant explique bien ce qu'il attendait.
- « Programmation objet, C++ »
  VB : Bien mais ca manque un peu de consistance → projet à la fin au lieu d'un exam
- « Technique de recherche d'emploi » et plus généralement rôle du SOIE
  SD/SB : Question importante car à partir de l'an prochain c'est les composantes qui devront les payer et les organiser
  VB : TB contrairement à l'an dernier probablement a cause de l'intervenant qui était plus proche. Forum pas grandiose et pas les bonnes entreprises/intervenants.
  SD : Pour le forum, l'UFR devra aussi payer, donc je note que ca ne vaut pas le cout, contrairement au TRE.
- « Anglais »
  SD : plus de problème d'emploi du temps parce qu'on les a mis avec les SSI
  VB : OK mais l'intervenante n'était pas prof et ca se voyait, meme si elle était americaine. But = passer le CLES et c'était correct pour çà.
  Tout le monde : le CLES c'est inconnu, ce serat mieux le TOEIC ou le TOEFL. Il faut faire remonter que c'est pas parce qu'on parle bien anglais qu'on peut etre prof d'anglais.
  SD/SB : voir si on ne peut pas faire financer quelques inscriptions au TOEFL par le labex.
- « Protection de contenu »
  VB : Pas très concluant car pas assez de crypto et trop de traitement du signal. Doerr a fait 2 fois le même cours et du coup le cours spécifique etait inutile par contre le TD spécifique OK. Ca reste vague, OK pour la culture
  SD : c'est important d'avoir des notions de traitement du signal et c'est le but des interventions de Doerr. Par contre il faut corriger le bug de dedoublement de cours

- « Protection de la vie privée »
  VB : TB
  SB : les étudiants de SSI le trouvent TB aussi
- « Cryptographie quantique »
  VB : OK
  SD : il doit faire pas mal de rappels mais ca ne sera plus le cas dans l'avenir grâce au nouveau cours de proba en M1.

<u>On enchaine sur le semestre 2 puisqu'il est terminé</u>

- « Codes correcteurs avancée »
  VB : TB
  SD : Carlach ne fait plus qu'une petite partie du module. L'autre partie est assurée par son doctorant à Orange. Ce changement d'intervenant a l'air positif.
- « Carte à puce »
  VB : cours OK, evaluation sympa (articles). Par contre ce cours arrive trop tard par rapport aux entretiens car il y avait beaucoup de stages sur les thèmes abordés dans ce cours.
  SD : Ce cours sera mutualisé à partir de l'an prochain avec les SSI. On peut donc en profiter pour le mettre sur Décembre-Janvier comme les autres modules de SSI.
- « Environnement économique et juridique de l'entreprise »
  VB : culture generale, OK

<u>Point sur les stages</u>

SD : Tout le monde a un stage. Ca s'est décanté fin janvier
SB : idem en SSI
VB : Ce qui manque, par rapport aux autres candidats sur les stages, c'est des projets.
SD : Il y en a déjà pas mal (AES, DSA, projet tutoré, prog C, CAP). Tout le monde ne s'est pas coltiné le FIPS 197 pour implémenter l'AES. Mais il faut les mettre en valeur (CV, entretien). Ca a déjà été dit mais il faut donc le dire plus souvent et insister encore plus sur l'importance de ces projets dans la formation même si ils ne sont pas tous notés. Eventuellement rajouter SHA-3 quand ce sera sorti.
SD:L'an dernier il y avait eu une reunion en fevrier pour expliquer ce qu'on attendait du stage. Cette année j'ai oublié. J'enverrais donc un petit topo par mail.

<u>Association des anciens étudiants</u>

Ca s'est finalement organisé autour d'un groupe facebook privé.
Le représentant des étudiants au comité (ou un autre si ils se mettent d'accord) inscrit les M2 en debut d'année et les M1 qui en font la demande.
Ca marche dejà pas mal : annonces de stage, entraide pour des contacts (Valentin Peltier a trouve un stage de M1 comme ca). Par contre ce n'est pas fait pour poser des questions sur le cours.

<u>Bilan du premier semestre de M1</u>

- « Algorithmique de base »
  KR : interessant. Corrigé en ligne des TP, c'est bien, par contre light en TD.
  FFT un peu rapide, pas de lien entre les 2 intervenants.
- « Algèbre de base »
  KR : tres rigoureux et structuré. Très dur et manque de corrections en TD
  ANAR indispensable
  SD : il y aura l'an prochain un preparcours crypto dans le parcours ingenieur incluant ANAR,
- « Théorie des nombres »
  KR : interessant, un peu trop magique, pas assez structuré.
  SD : visiblement, le programme n'a encore pas été fait en entier, comme les années précédentes,
- « Programmation C »
  KR : Intervenant pas terrible (fautes, cours pas au point, pas de TP de preparation du projet d'algèbre et pas clair qu'il fallait faire les 2 projets). Module trop court.
  SD : L'an prochain le module passera à 6 ECTS mais sera plus orienté calcul numérique. **PL** envoie des idées de poit à rajouter au programme plus spécifiqe à la cryptographie.
- « Probabilités et statistiques pour l'ingénieur (PSIN)»
  KR : prof bien. Toujours pas de stats.
  SD : Ce module disparaît l'an prochain (plus précisement, il passe en L3) et est remplacé par un module plus orienté vers la formation. Le programme reste d'ailleurs à faire. Je vais envoyer une première version et **DA/PL** me feront des commentaires dessus et des propositions de sujets à traiter.
- « Anglais »
  KR : Ca va (Nicolas André semble plaire à tout le monde) mais tout le monde ne participe pas.

  KR : Globalement pas assez de cryptographie.
  SD : C'est normal au premier semestre car la plupart des modules sont des modules du Master de mathématiques. L'an prochain la partie de THIN sur les codes correcteurs sera au premier semestre.

<u>Présentation des parcours à partir de l'an prochain</u>

SD présente la nouvelle habilitation gràce au tableau ci dessous (en grisé ce qui change)

Nouvelle maquette de Master (2012-2016)

Spécialité Mathématiques de l'information, cryptographie

	CM	TP	TD	ECTS	Remarque
Semestre 1					
Algèbre de base	36	6	36	9	
Algorithmique de base	24	12	24	6	
Programmation scientifique 1	18	18	12	6	Mutualisé avec le M1 de modélisation
Théorie des nombres	24	6	24	6	
Codes correcteurs	12	8	8	3	Partie 1 de THIN actuel
Insertion professionnelle			10	0	En partenariat avec le SOIE
Semestre 2					
Cryptographie	24	12	24	6	Partie 2 de THIN actuel
Probabilités pour la théorie de l'information	24		24	6	Module spécifique à créer
Complexité	12		12	3	Partie « complexité » de LTMC actuel, la partie logique pourra être prise en surnuméraire
Algèbre commutative et géométrie algébrique	24	6	24	6	
Anglais			30	3	
projet tutoré ou stage				6	
Semestre 3					
Recherche d'emploi, recherche de stage			10	0	En partenariat avec le SOIE
Cryptographie avancée	24	12	12	6	
Mathématiques de la cryptographie	24		24	6	
Systèmes d'exploitation, réseaux informatiques, sécurité	24	24		6	
Autour de l'authentification ou	16	16		3	Les 5 premières UE sont mutualisées avec la spécialité SSI du master d'informatique
Contrôle d'accès ou	14	10	8		
Vote électronique ou	24		8		
Détection d'intrusion ou	20	12			
Protection de la vie privée ou	16	16			
Protection de contenus	10		12		Cours mutualisé avec la spécialité Recherche du master d'informatique.
Programmation objet, C++, les bases	12	12		3	Mutualisé avec le M2 de modélisation
Programmation avancée pour la cryptographie	12	12		3	
Anglais			30	3	
Séminaire				0	
Interventions de professionnels				0	
Semestre 4					
Codes correcteurs avancés	12		12	3	
Cartes à puces	20		12	3	Mutualisé avec la spécialité SSI du master d'informatique.
Environnement économique et juridique de l'entreprise	12		12	3	
Autour de l'authentification ou	16	16		3	
Contrôle d'accès ou	14	10	8		Mêmes choix qu'en semestre 3 sauf que Protection de contenus est remplacé par cryptographie quantique
Vote électronique ou	24		8		
Détection d'intrusion ou	20	12			
Protection de la vie privée ou	16	16			
Cryptographie quantique	12		12		
Stage				18	
Séminaire				0	
Interventions de professionnels				0	