Compte rendu du stage de l'ENSEA des 12 et 13 mai 2015

L'ENSEA, à l'initiative des Professeurs Patrick David et Philippe Bouafia, a proposé un stage Liesse sur la cryptologie. Treize enseignants de CPGE (et deux enseignants de l'ENSEA) se sont ainsi retrouvés mardi 12 et mercredi 13 mai à Cergy.

Accueillis par Patrick David, ils ont reçu un mot de bienvenue de Madame Hafemeister, Directrice de l'ENSEA, avant de plonger sans attendre dans leurs études.

Mardi matin, Patrick David a présenté les deux versants de la cryptologie :
- la cryptographie (les procédures de chiffrement et de déchiffrement)
- la cryptanalyse (conception de méthodes d'attaque, évaluation de la résistance d'un chiffrement)
ainsi que les deux catégories de clés (symétrique ou asymétrique) et la « préhistoire » de la discipline (jusqu'à 1970) basée sur les clés symétriques. Il a ensuite dirigé des activités statistiques utiles pour attaquer ce type de chiffrement.

L'après-midi, Philippe Bouafia a pris le relais pour exposer les détails du DES (Data Encryption Standard) qui a été utilisé de 1975 à 2000, puis des notions de cryptanalyse différentielle intervenant dans des stratégies d'attaque. Enfin, il a animé une séance de travaux dirigés sur ces deux thèmes.

Mercredi matin, Patrick David a détaillé les exigences du RSA dans le choix de la clé si on veut qu'elle résiste aux attaques de Fermat et de Wiener. Le problème du choix de grands nombres premiers « robustes » a conduit à implémenter le test probabiliste de primalité de Rabin-Miller et à parler de fractions continues.

L'après-midi, Philippe Bouafia a présenté la notion de fonction de hachage et diverses applications puis guidé l'attaque du chiffrement par SHA1 de mots de passe faibles, avant de faire étudier une fonction de hachage par logarithme discret.

Les organisateurs avaient préparé à leur auditoire un environnement de travail idéal (cours en powerpoint, travaux dirigés avec Ipython notebook) et ont réussi à rendre clair un sujet aussi austère (voire rébarbatif) que le DES. Les participants au stage ont beaucoup apprécié l'alternance de présentations théoriques, de test et d'exercices de codage en Python. L'effort de sobriété dans la syntaxe Python aussi.

Nous les remercions de nous avoir épargné tout souci matériel, en réservant des repas au restaurant d'entreprise tout proche au cours desquels nous avons pu échanger nos points de vue respectifs. Patrick David notamment, qui s'est rendu disponible pendant l'intégralité du stage, et qui a guidé une brève visite des locaux, a présenté les contours de l'Institut Polytechnique du Grand Paris (qui regroupe l'ENSEA, l'EISTI et SUPMECA depuis peu) mais a aussi parlé de rencontres humaines qui l'ont marqué lors de l'accueil et de l'encadrement d'étudiants étrangers.

Au nom de l'UPS, je remercie l'ENSEA de nous avoir offert cette formation de grande qualité, tant sur le plan technique que culturel. Je pense me faire l'interprète de tous les auditeurs en formant le souhait que ce stage très enrichissant puisse être proposé dans les années à venir.

Daniel Lecouturier, Charlotte Dézelée et Eliane Gayout