Cergy, le 17 janvier 2012

ENSEA-Cergy 95 Département Signal et Télécommunications (http://www.ensea.fr/)

Stage LIESSE :Cryptologie

Date : 4 séances sur deux journées, lundi 14 et mardi 15 mai 2012

Objectif du stage

Présentation des principales classes de méthodes classiques et "modernes " de cryptage et des outils mathématiques associés. Applications, divers contextes.
Étude des attaques possibles, mise en oeuvre avec Mathematica du cryptage et décryptage.

Chaque séance comprendra une partie de travaux personnels sur machine, sous Mathematica 7, avec des outils de démonstration donnés, et leur utilisation pour résoudre les exercices.
Déjeuner organisé à proximité.

9 h -12 h	P. David, professeur de Mathématiques et Informatique

1- 1.1 Historique : Décalages, permutations, substitutions

1.2 Cryptographie classique (codes linéaires,Vigenere,Hill) et ses faiblesses

1.2.2 Attaque des codes classiques. Statistiques lexicales, indice de concordance.

1.3.1 Le standard DES (codage symétrique à clé secrète, non-linéaire)

1.3.2 Les attaques sur le DES. Notions sur le standard AES.

13 h 30 -17 h	M.Michaut, professeur de Mathématiques et Traitement du Signal

2- 2.1 Cryptage et complexité. Critères de sécurité des codes.

2.2 Outils de théorie des nombres : primalité, factorisation, arithmétique modulaire, Fractions continues, Théorème du reste chinois…

2.3 Primalité et Factorisation

2.4 Courbes elliptiques, Factorisation par ECM

9 h -12 h	P.David

3- 3.1 Systèmes à clé publique : RSA, variantes, contextes d'utilisation

3.2 Faiblesses du RSA, conditions de mise en oeuvre efficace

3.3 Un exemple : l'attaque de Wiener,l'attaque de Wiener étendue

3.4 Le domaine de sécurité du RSA

13 h 30 -16 h30	F.Michaut

4-Cryptage par les exponentielles modulaires

4.1 Signature El Gamal et problème du Logarithme discret

41.1 Principe, notion de signature, exponentielle modulaire

41.2 Attaques : « Baby step, Geant step », Pohlig-Hellman

4.2 Cryptage par les courbes elliptiques

16 h 30 -17 h Bilan du stage

Contact à l'ENSEA : F. Michaut et P. David Département Signal et Télécommunications
Tél: 01-30-73-66-66 Courriel : michaut@ensea.fr et david@ensea.fr
École Nationale Supérieure de l'Électronique et de ses Applications
6 Avenue du Ponceau 95000 Cergy