JOURNEE SCIENTIFIQUE DE LA FEDERATION CHARLES HERMITE

« CRYPTOGRAPHIE ET THEORIE DES NOMBRES »

VENDREDI 22 JUIN 2012 - IECN - SALLE DE CONFERENCES - 2EME ETAGE

PROGRAMME DE LA JOURNEE

- 9:15 – Accueil
- 9:30 – **Damien Stehlé** (LIP, Ecole Normale Supérieure de Lyon)
  - **« Une preuve de sécurité pour le cryptosystème NTRU »**
- 10:15 – Pause café
- 10:45 – **Alain Plagne** (CMLS, Ecole Polytechnique, Palaiseau)
  - **« De la combinatoire additive à la théorie des codes, grâce à Davenport »**
- 11:30 – **Emmanuel Thomé** (LORIA)
  - **« Computing Igusa class polynomials with the complex analytic method »**
- 12:15 – Pause déjeuner
- 14:15 – **Jie Wu** (IECN)
  - **« Courbes elliptiques et cryptographie »**
- 15:00 – Pause-café
- 15:15 – **Claus Fiecker** (Fachbereich Mathematik, Universität Kaiserslautern)
  - **« New Ideas for the computation of Class Groups »**
- 16:00 – **Gérald Tenenbaum** (IECN)
  - **« Sur les modèles probabilistes de l'arithmétique »**