dapnia
cea
saclay

# SÉMINAIRE du SPP

**David Pointcheval**
(ENS Paris)

# La cryptographie et la sécurité concrète

La cryptographie est à la fois un art très ancien, et une science très jeune. Pour ce qui est de la sécurité concrète, les résultats sont très récents.

Dans cet exposé, nous ferons un rappel historique pour présenter les évolutions des mécanismes cryptographiques. Mais la formalisation théorique des problèmes de sécurité a moins de 30 ans, avec l'avènement de la cryptographie asymétrique. Une recherche foisonnante a en effet trouvé ses racines au sein de la théorie de la complexité, qui a modélisé la sécurité, mais avec des analyses asymptotiques.

Ces dernières années ont vu se développer la notion de « sécurité trouvée », qui s'attache à étudier la sécurité de schémas concrets et efficaces, tout en permettant une interprétation effective quant à la taille des paramètres à utiliser en fonction du niveau de sécurité souhaité. Nous retracerons ces différentes étapes, avec quelques exemples.

## Lundi 26 mars 2007 à 15 heures

## Salle André Berthelot, bât. 141

Le café sera servi 15 minutes avant

NB : *La présentation d'une carte d'identité ou d'un passeport est exigée à l'entrée du centre. Tous les auditeurs extérieurs sont priés de prévenir à l'avance de leur visite Emilie Chancrin, tél. 01 69 08 23 50 (U.E. : délai de 24 h, hors U.E. : délai de 4 jours).*