REUNION RTP 13 AS NOUVELLES TENDANCES EN CRYPTOGRAPHIE
Lundi 29 Septembre à 14 heures en C.229.
Trois exposés:

Capacities of graphs and digraphs

Janos Korner, "La Sapienza University", Rome (Italy)

Sperner capacity is a natural generalization of Shannon capacity from graphs to directed graphs. In combinatorics, it has proved to be a valuable tool to obtain asymptotically tight estimates for several hard problems in extremal set theory. Some of these results have found exciting applications in computer science.

Yet the precise value of Sperner capacity is very hard to determine even for some orientations of the edges of a complete graph. Improving on earlier bounds of Calderbank et al., Blokhuis and Noga Alon, we introduce a novel upper bound for the Sperner capacity of arbitrary digraphs. Our bound, obtained in joint work with Concetta Pilotto (Rome) and Gabor Simonyi (Budapest), is based on a suitable generalization for directed graphs of the concept of "local chromatic number", as defined by Erdos, Furedi, Hajnal, Komjath, Rodl and Seress (1986).

The exposition will be self-contained. In particular, the first part is a survey on Shannon's graph capacity and our generalization to directed graphs; Sperner capacity.

Codes séparants

Hugues Randriam, ENST

On expose diverses constructions et bornes existentielles sur les codes séparants, en insistant notamment sur la construction par Xing de bons codes issus de la géométrie algébrique.

Identification et révocation par codes séparants

Gérard Cohen et Gilles Zémor

Le contexte est le suivant. Un flot de données (une émission) est chiffré par une clé de session appelée S. Ce flot est précédé par un *en-tête* $F(S)$, qui contient la clé de session S chiffrée par une fonction F. La fonction de chiffrement est choisie de manière à admettre un grand nombre N de fonctions (ou clés) de déchiffrement, égal au nombre d'utilisateurs du système.

On distingue deux préoccupations du diffuseur: l'*identification* des décodeurs et la *révocation*. On montre comment l'emploi de codes séparants permet de les traiter.