# Y’a d’la crypto dans l’air…

Nombre minimal d’étudiants : 3 très motivés par un projet « main dans le cambouis » !

L’objectif de ce projet est d’étudier la sécurité des communications opérées par téléphones mobiles.

Deux études de natures différentes seront demandées aux étudiants. Une première sera de revoir et d’implanter une attaque sur les cryptosystèmes utilisés dans les premières versions des protocoles utilisés dans nos téléphones mobiles. Ces attaques nécessitent des techniques de calcul distribué pour pouvoir être menées à terme (suivre HPC est donc un plus voire une nécessité). Nous demanderons aux étudiants, avant de passer à une phase d’implantation, d’analyser finement les besoins d’une telle attaque en pratique (voir [1]).

Une seconde étude (qui pourra être effectuée en parallèle de la première) s’intéressera aux protocoles de communications hertziennes utilisés par nos mobiles. Pour ce faire, les étudiants devrons se familiariser avec du matériel d’analyse de spectres, de réception et émission radio open source de type USRP. Une première étape de base sera par exemple de réaliser un récepteur FM ou GSM avec GnuRadio et un USRP B210 (voir [2]). Les étudiants devront ensuite monter une démonstration d’utilisation de l’outil OpenBTS.

En guise de conclusions, les étudiants devront nous donner leur avis et présenter les précautions d’usage en matière de sécurité pour les réseaux mobiles.

[1] : http://en.wikipedia.org/wiki/A5/1

[2] : https://www.youtube.com/watch?v=cygDXeZaiOM