# Cryptologie Embarquée

L'objectif principal de ce projet est de se familiariser avec la programmation et l'analyse d'implémentations cryptologiques sur plateformes embarquées.

La première étape de ce projet sera l'étude et l'implémentation d'un algorithme cryptographique. Le contexte de développement sera particulier puisque la cible sera une puce très simple. L'étudiant devra donc se familiariser avec l'environnement de développement et l'architecture considérée (AVR).

La seconde partie sera consacrée à l'analyse de cette implémentation par canaux auxiliaires. Plus exactement, l'étudiant essaiera de retrouver la clé secrète utilisée dans l'implémentation cryptographique en utilisant des mesures de courant.

Moyens à disposition :

L'étudiant sera amené à utiliser une plateforme de test ChipWhisperer permettant à la fois de programmer un chip AVR et de réaliser une analyse par consommation de courant.

Contact :

Guénaël Renault (guenael.renault@lip6.fr)