Une situation didactique en cryptographie débranchée

Simon Modeste, Iro Bartzia

Dans cet atelier, nous présentons une situation d'informatique débranchée en cryptographie. Le protocole présenté est un protocole de cryptographie asymétrique, basé sur un problème « difficile » en théorie des graphes.

Le système de cryptographie est déjà connu en tant qu'activité débranchée, et notre principale contribution est l'organisation et l'analyse de l'activité à l'aide des outils de la Théorie des Situations Didactiques (variables didactiques, milieu).

Après avoir rappelé ce qu'est la cryptographie asymétrique et présenté le protocole lui-même, nous proposerons aux participants de vivre l'activité elle-même. Dans un second temps, nous échangerons sur les analyses des apprentissages possibles, et les choix d'organisation de la situation.

Nous avons expérimenté cette situation dans différents contextes, et nous pourrons échanger sur les retours d'expérience et la mise en œuvre de cette situation en contexte d'enseignement, ou de formation d'enseignants.