Comment garder un secret? Premiers pas en cryptographie.

De nos jours, une grande partie de nos communications se fait de manière électronique, au travers des ordinateurs, téléphones, tablettes... Ces communications sont protégées pour qu'une tierce personne ne puisse pas intercepter le contenu des messages. Ainsi, les messages qui transitent par ces canaux sont chiffrés: ils sont 'traduits' dans un langage indéchiffrable pour toute personne étrangère à la communication. L'ensemble de ces techniques de protection des communications s'appellent la cryptographie.

Dans ce sujet, nous présenterons les deux étapes fondamentales de la cryptographie: le codage (transformer un texte en nombres), et le chiffrement proprement dit. Ces techniques seront illustrées par un exemple de système de codage/chiffrement basé sur le calcul du reste pour la division euclidienne. Nous présenterons également les limites de ce chiffrement.