UNIVERSITÉ DE NEUCHÂTEL

Faculté des sciences
Institut de Mathématiques
Rue Emile-Argand 11
2000 Neuchâtel, Suisse
Tél: + 41 (0)32 718 2800
Email : secretariat.math@unine.ch

SEMINAIRE MATHEMATIQUES ET SOCIETE

Mercredi 6 décembre 2017 à 16h15

Auditoire Louis-Guillaume, ALG, F200

Conférencier : Prof. David-Olivier Jaquet-Chiffelle
Université de Lausanne

« Cryptanalyse du Code de Vigenère »

Résumé : Le code de Vigenère est un algorithme de chiffrement qui fut considéré historiquement comme incassable. Les Confédérés américains l'ont utilisé pendant la guerre civile dans les années 1860. Aujourd'hui, on sait comment attaquer le Code de Vigenère. Il existe toutefois une exception : lorsque la clé est parfaitement aléatoire et aussi longue que le texte à chiffrer, on obtient le chiffre de Vernam qui, lui, est réellement incassable… D'ailleurs, cette version du Code de Vigenère redevient d'actualité avec l'avènement de la cryptographie quantique.
La cryptanalyse du Code de Vigenère illustre et fait ressortir plusieurs principes fondamentaux de la cryptanalyse qui restent valides en 2017. Différents outils mathématiques seront présentés ; ils relient « invariants » de la langue naturelle, statistique, probabilité et géométrie dans l'espace pour extraire les propriétés de la clé de chiffrement.

Organisation : **Paul Jolissaint**
Institut de Mathématiques
Emile Argand 11
2000 Neuchâtel