Leçon inaugurale

Courbes et cryptographie : les mathématiques au service de la sécurité informatique

La cryptographie au début se préoccupait de la conversion des messages en groupes de chiffres illisibles, pour protéger le contenu du message pendant son transport d'un endroit à l'autre.

A l'ère moderne, le développement de la technologie a créé le besoin pour la cryptographie de passer de la confidentialité des messages à davantage de fonctionnalités, comme le contrôle de l'intégrité des messages, l'authentification de l'identité de l'émetteur/récepteur, et les signatures digitales. Ces applications plus sophistiquées vont de pair avec la nécessité d'utiliser des techniques mathématiques avancées pour les réaliser.

Ces dernières années, la méthode de la cryptographie à clé publique a été largement adoptée. Dans ce contexte, nous basons la sécurité sur des problèmes mathématiques difficiles, en s'appuyant sur le fait que ces problèmes ne peuvent pas être résolus pratiquement, même en utilisant les meilleurs ordinateurs. Certains de ces problèmes proviennent de la théorie mathématique des courbes.

UNIVERSITÉ DE NEUCHÂTEL

FACULTÉ DES SCIENCES

Professeure
Elisa Gorla

Chaire de mathématiques appliquées

La leçon inaugurale aura lieu
le **mercredi 26 novembre 2014** à 18h15
Aula d'Unimail, rue Emile-Argand 11