

**Institut de Mathématiques**

Rue Emile-Argand 11

CH-2000 Neuchâtel

## **SEMINAIRE MATHÉMATIQUES ET SOCIÉTÉ**

**Mercredi 9 mai 2012, à 16h15**

**Aula Unimail, F0100**

Conférencier : Jean Monnerat (SwissSign AG)

***“Les mathématiques de la SuisseID”***

Résumé : Introduite en 2010, la SuisseID est la première carte d'identité électronique standardisée de Suisse. Elle permet à son détenteur d'accéder de manière sécurisée à divers services en ligne. Une telle technologie serait irréalisable sans les techniques de cryptographies modernes reposant sur la théorie des nombres. Le présent exposé présentera les bases cryptographiques et mathématiques nécessaires à la conception de la SuisseID. Certains aspects algorithmiques et de sécurité de ces mécanismes cryptographiques seront également abordés. Enfin, nous exposerons le concept de certificat numérique, élément central permettant la création d'une identité électronique à partir d'une identité physique.

Organisation : Paul Jolissaint  
Institut de Mathématiques  
Emile-Argand 11  
CH – 2000 Neuchâtel