L'algorithme RSA

Conférencier : Guillaume Lavoie
Où : Z-205 pav. McNicoll
Quand : Mercredi 30 septembre 12 :30 à 13 :30

Résumé : Lorsque vous envoyez un courriel à vos amis, qu'est-ce qui vous garantit que personne à part eux ne peut le lire? Quand vous faites un achat par carte de crédit sur internet, qui vous assure que vous n'êtes pas en train de donner l'accès à votre compte bancaire au premier venu au lieu de payer? Dans l'ère de l'électronique, il est courant d'envoyer des informations personnelles sur le web et on veut évidement pouvoir le faire en toute sécurité. Si c'est maintenant possible d'y arriver, c'est grâce à l'algorithme RSA, une méthode d'encodage à clé publique.

Nous commencerons par une brève introduction aux principes de base de la cryptographie, puis nous verrons comment l'algorithme RSA permet de garantir la confidentialité des multiples échanges par internet. Nous verrons à quel point la méthode actuelle est sécuritaire et quelles en sont les failles, les limites et les incovénients.