Théorie des nombres et cryptographie : l'algorithme RSA

Description

La cryptographie a pour but le développement et l'analyse de méthodes et techniques pour chiffrer des informations. Ayant ses origines dans l'antiquité, la cryptographie est devenue indispensable dans l'ère numérique, où des milliers de transactions bancaires et commerciales sont faites toutes les minutes sur internet. Tout transfert de données sensibles nécessite des méthodes permettant de sécuriser et de protéger la communication.

Une des méthodes de cryptographie les plus répandues de nos jours est le chiffrement RSA. Comme tout système de cryptage à clé publique (ou asymétrique), le fonctionnement du RSA est basé sur une paire de deux clés différentes. La première est « publique », c'est-à-dire accessible à tout le monde et est utilisée pour chiffrer les messages. La seconde est « secrète », c'est-à-dire qu'elle n'est connue que par le destinataire des messages et est utilisées pour les déchiffrer. En pratique, ces clés consistent en de très grands nombres entiers spécifiques et le chiffrement et déchiffrement d'un message se font à l'aide d'opérations mathématiques ingénieuses mais élémentaires qui sont fondées sur la théorie des nombres et le calcul de reste pour la division euclidienne.

Le stage a pour objectif premier de comprendre le fonctionnement du chiffrement RSA en détails, ainsi que les mathématiques sous-jacentes. Un deuxième objectif est de réaliser une implémentation de l'algorithme sur ordinateur. Le stage se clôturera par une présentation par les élèves expliquant le chiffrement RSA et d'une démonstration de leur implémentation numérique.

Prérequis

- Être familier avec un langage de programmation (p.ex. Matlab ou Python).
- Aucune notion hors programme du lycée n'est strictement requise.
- Goût pour les mathématiques, capacité d'auto-apprentissage.

Public

- Accessible à partir de 16 ans (selon CV).
- Doit être réalise par groupe de deux (candidature isolée encouragée).

Encadrement

Le stage se déroulera au sein de l'unité de recherche en mathématiques de l'Université du Luxembourg (à Belval). Il sera encadré par un/e chercheur/euse en mathématiques.

Durée

- 5 jours

Contact

- thierry.meyrath@uni.lu

SCIENTEENS LAB
DE LABO FIR JONKER

UNIVERSITÉ DU LUXEMBOURG

RMATH | MATHEMATICS RESEARCH UNIT