Lehrstuhl D für Mathematik
Lehrstuhl für Mathematik (Algebra)
Dr. T. Hanke
Dr. M. Wibmer

29. Januar 2013

Seminar zur Kryptographie
Seminar zur Algebra I
SS 2013

Referenz: MSMath-553, BSMath10-375

Zeit und Ort: Mi, 17:30 – 19:00, H 212 (ab 10.4.2013)

Beschreibung: Die Kryptographie beschäftigt sich allgemein mit dem Thema der Informationssicherheit, und speziell mit dem Design von Systemen des Informationsaustausches, die resistent sind gegen unerwünschtes Lesen und Verändern. Hierfür notwendige mathematische Methoden bilden den Inhalt dieses Seminars. Die Studierenden sollen ein spezielles Thema aus der Literatur selbstständig erarbeiten und präsentieren, was in der Regel die mathematischen Grundlagen sowie eine reale Anwendung in der modernen Kommunikationstechnik umfasst.

Teilnehmer: Master- und fortgeschrittene Bachelor-Studierende aus Mathematik und Informatik mit Anwendungsfach Mathematik.

Inhalte: Informationstheorie, Pseudo-Zufallszahlen, Public Key Kryptographie-Verfahren, Secret Key Kryptographie-Verfahren, Primzahltests, Elliptische Kurven, Authentifikationssysteme, Schlüsselaustausch, Zero-Knowledge Beweise

Organisatorisches: Unverbindliche Voranmeldung unter Angabe von Fachsemester und Studiengang bitte bis zum 8.2.2013 an `hanke@math.rwth-aachen.de`. Genauere Informationen zu den verfügbaren Themen und zur Vorbesprechung werden anschließend per email und über die Webseite bekannt gemacht.

Prüfungsleistung: Regelmäßige Teilnahme und Vortrag mit schriftlicher Ausarbeitung.

Webseite: `http://www.math.rwth-aachen.de/~Timo.Hanke/krypto13.html`