Leibniz Universität Hannover
Fakultät für Mathematik und Physik
Institut für Algebraische Geometrie

Januar 2016

PROSEMINARANKÜNDIGUNG

für das Sommersemester 2016

Thema: Kryptographie (2S)

Veranstalter: apl.Prof. A. Frühbis-Krüger, Dr. Bernd Schober

Voraussetzungen: Kenntnisse etwa im Umfang von Linearer Algebra I und Computeralgebra

Literatur:

1. Beutelpacher,A., Neumann,H., Schwarzpaul,T.: Kryptographie in Theorie und Praxis, Vieweg Verlag Wiesbaden (2005)
2. Beutelspacher,A.: Kryptologie, Vieweg Verlag Wiesbaden (2005)
3. Beutelspacher,A., Schwenk,J., Wolfenstetter,K.: Moderne Verfahren der Kryptographie, Vieweg und Teubner Verlag Wiesbaden (2010)
4. Buchmann,J.: Einführung in die Kryptographie, Springer Verlag Berlin (1999)
5. Karpfinger,C., Kiechle,H.: Kryptologie, Vieweg und Teubner Verlag Wiesbaden (2010)

Überblick:

Gerade in der heutigen Zeit weltweit vernetzter Computer stellt die Verschlüsselung von Daten eine zentrale Technologie dar, der wir überall begegnen – vom Geldautomaten über E-Mail bis zum Einloggen im StudIP. Das Herzstück moderner Verschlüsselungsverfahren bildet die Mathematik, insbesondere Kenntnisse aus der Algebra und Zahlentheorie finden hier Anwendung. Daher werden wir uns in diesem Seminar zuerst mit der gezielten Erarbeitung der entsprechenden Grundlagen beschäftigen, ehe wir dann auch praktisch relevante Algorithmen wie z.B. das AES-Verfahren oder den Diffie-Hellman-Schlüsselaustausch kennenlernen. Die zugrunde liegende Literatur ist durchgehend für Studierende der ersten beiden Studienjahre

in Studiengängen der Mathematik und Informatik geschrieben.
Einige der späten Themen sind auch als Vorbereitungsseminar auf das Anfertigen einer Bachelorarbeit (FBa) in diesem Gebiet denkbar.

unverbindliche Vorbesprechung: 1.2.2016, 16:00 Uhr, 1101-G116 (Blaue Grotte)
Anmeldung: bei der Vorbesprechung oder per Mail an schober@math.uni-hannover.de