Leibniz Universität Hannover
Fakultät für Mathematik und Physik
apl. Prof. Dr. Thorsten Holm

Juli 2020

Seminar für FüBa-Studierende
Kryptographie
Wintersemester 2020/21

Die Kryptographie ist die Wissenschaft der Verschlüsselung von Informationen und beschäftigt sich heutzutage auch mit dem Schutz von Daten, Nachrichten und Übertragungskanälen. Viele kryptographische Verfahren basieren essentiell auf mathematischen Methoden aus der Algebra, Zahlentheorie und Geometrie. In diesem Seminar werden wir einige der wichtigsten Verfahren und deren mathematische Hintergründe studieren, Themen sind z.B. das RSA-Verfahren, das El Gamal-Verfahren, Primzahltests, Diskrete Logarithmen, das Diffie-Hellman-Verfahren, Hash-Funktionen, Digitale Signaturen.

Literatur: Als Grundlage für die Vorträge im Seminar werden wir einzelne Kapitel aus verschiedenen Lehrbüchern nutzen, z.B. aus

J. Buchmann: *Einführung in die Kryptographie* (Springer Spektrum)

N. Koblitz: *A Course in Number Theory and Cryptography* (Springer Graduate Texts in Mathematics)

S. Rubinstein-Salzedo: *Cryptography* (Springer Undergraduate Mathematics Series)

Adressatenkreis: Das Seminar richtet sich ausschließlich an Studierende des fächerübergreifenden Bachelorstudiengangs. Nach erfolgreicher Teilnahme vergebe ich gerne Themen für Bachelorarbeiten.

Voraussetzungen: Kenntnisse aus den Vorlesungen des ersten Studienjahres und aus der Vorlesung Algebra I.

Termin des Seminars: Durch die Corona-Einschränkungen ist es derzeit noch nicht klar, wann und in welcher Form das Seminar stattfinden kann. Wenn möglich, soll das Seminar natürlich als Präsenzveranstaltung stattfinden, wöchentlich oder eventuell auch als Blockveranstaltung am Ende des Semesters. Das Seminar findet aber auf jeden Fall statt, notfalls in Form von Videokonferenzen.

Anmeldung und Vergabe der Themen: Interessierte melden sich bitte direkt bei mir per email an, unter `holm@math.uni-hannover.de`. Bitte dabei Namen, Matrikelnummer, Studiengang und Fachsemester angeben. Nach Eingang der Anmeldungen werden die Themen in Absprache mit den Teilnehmenden vergeben.