Proseminar:	**Kryptographie**
Dozentin:	**Prof. Dr. Heike Mildenberger**
Zeit/Ort:	**Blockseminar nach dem Praxissemester, Januar, Februar oder vorlesungsfreie Zeit**
Tutorium:	**Dr. Maxwell Levine**
Vorbesprechung:	**Mo, 18.7.2022, 13:00 Uhr, SR 404**
Teilnehmerliste:	E-Mail an heike.mildenberger@math.uni-freiburg.de vor dem 13.7.2022
Web-Seite:	`http://home.mathematik.uni-freiburg.de/mildenberger/veranstaltungen/ws22/kryptographie.html`

Inhalt:

> ... both Gauss and lesser mathematicians may be justified in rejoicing that there is one science [number theory] at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean.

— G. H. Hardy, *A Mathematician's Apology*, 1940

Hardy wäre überrascht und vielleicht unzufrieden über die heutige Nähe der Zahlentheorie zum Alltag. Fehlerkorrigierende Codes und kryptographische Verfahren gehören zum möglichst sicheren und geheimen Informations- und Geldtransfer über das Internet.

Im Seminar studieren wir unter anderem Public-Key-Verfahren wie zum Beispiel die unter ihrem Namen bekannten Diffie-Hellman- und Rivest-Shamir-Adleman-Verfahren. Neben der Zahlentheorie spielen Algebra, Komplexitätsabschätzungen und probabilistische Algorithmen eine Rolle.

Wie es zur Kodierung gehört, sind die genannten Lehrbücher als PDF-Dateien mit Login über die Universitätsbibliothek erhältlich.

Literatur:

1.) Albrecht Beutelspacher, Heike Neumann, Thomas Schwarzpaul, Kryptografie in Theorie und Praxis, 2. Ed., Vieweg + Teubner, 2010.
2.) Johannes Buchmann, Introduction to Cryptography, Second Edition, Springer, 2004, (auch auf Deutsch).
3.) Jeffrey Hoffstein, Jill Pipher, Joseph Silverman, An Introduction to Mathematical Cryptopgraphy, Second Edition. Springer, 2014.

Notwendige Vorkenntnisse:	Anfängervorlesungen
Nützliche Vorkenntnisse:	Algebra und Zahlentheorie, Stochastik
Studien-/Prüfungsleistung:	Die Anforderungen an Studien- und Prüfungsleistungen entnehmen Sie bitte dem aktuellen Modulhandbuch Ihres Studiengangs.
Prüfungsanmeldung:	Diese muss bei (Pro-)Seminaren bis zum Mittwoch vor Vorlesungsbeginn in HisInOne erfolgen.