

---

Vorlesungsankündigung für WS 2008/09

# Zahlentheorie, Algebra und Kryptografie

mittwochs 12.15 bis 13.45 Uhr Raum C 12.108

2 SWS, die Übungen werden integriert.

426848919408260889649017766380934114559426810216408632941886557063352775943181424423400235327944135499

106097044032117109032049048

Algebra und Zahlentheorie gehören zu den ältesten und tragenden mathematischen Disziplinen. Die Grundlagen sollen in dieser Vorlesung **anwendungsbezogen** erlernt werden. In der Kryptographie führen große Primzahlen und algebraische Methoden zu sicheren Verschlüsselungen mit öffentlichen Schlüsseln (public-key), zu Prüfcodes, No-Key-Verfahren, PIN und Datensicherheit.

Durch den Einsatz von CAS sollen Elemente entdeckenden Lernens eingebracht werden. Aber auch die sonst mühevollen Rechnungen sollen erleichtert werden. Im Hinblick darauf, dass CAS nun in die Richtlinien aufgenommen sind, kann dieses Thema auch in Schulen vermittelt werden. Kenntnisse über kryptographische Methoden gehören heute zur mathematischen Bildung.

$$2^2 \cdot 7 \cdot 8941$$

$$\begin{pmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \\ 7 & 11 & 1 & 5 \\ 11 & 7 & 5 & 1 \end{pmatrix}$$

Literatur:

Bartholomé u.a.: Zahlentheorie für Einsteiger,

Beutelspacher: Kryptologie, u.a. (Siehe mystudy)

51961524227066318805823390245176171008284157614311418841674209383557990507264001112434385602717457251

Auf den Internetseiten finden Sie Informationen.

<http://haftendorn.uni-lueneburg.de>

BA LBS, Fach Mathematik, Modul 2 Algebra (Info Internet s.o.)

Für GHR-Lehramt ist die in Ihrem Bereich angebotene "Algebra und Zahlentheorie" nicht durch diese Veranstaltung ersetzbar. Aber als Ergänzung (auch als Festigung vor dem Examen) ist sie sehr sinnvoll. BA Lehren und Lernen im Modul:

Elementarmathematik vertiefen.

Keine Voraussetzungen. Ab 1. Sem.

Die Übungen werden z.T. integriert und z.T. von höheren Semestern betreut.

Für Gasthörer und Schüler möglich.

Beachten Sie, dass diese Vorlesung erst SS 10 wieder angeboten wird.