Modulbezeichnung: **Kryptographie Lehramt (Kry L)** **5 ECTS**
(Cryptography for teaching students)

Modulverantwortliche/r: Wolfgang Ruppert
Lehrende: Wolfgang Ruppert

Startsemester: SS 2018	Dauer: 1 Semester	Turnus: unregelmäßig
Präsenzzeit: 45 Std.	Eigenstudium: 105 Std.	Sprache:

Lehrveranstaltungen:

Lehramts-Studierende koennen diese Veranstaltung mit 5 ECTS als Modul "Angewandte Mathematik" einbringen.
Kryptographie I (SS 2018, Vorlesung, 4 SWS, Wolfgang Ruppert)
Übungen zur Kryptographie I (SS 2018, Übung, 2 SWS, Wolfgang Ruppert)

Empfohlene Voraussetzungen:

Grundkenntnisse aus den Modulen Analysis I und Lineare Algebra I

Inhalt:

- Einführung in die Kryptographie
- Klassische Chiffrierverfahren
- Grundeigenschaften der Ringe Z und Z/nZ
- Primzahltests
- Public-Key-Kryptosysteme - RSA
- Die Pollard-rho-Methode zur Faktorisierung
- Kryptographische Anwendungen diskreter Logarithmen
- Kryptographische Hashfunktionen
- Digitale Signaturen
- Methoden zur Berechnung diskreter Logarithmen
- Enigma

Lernziele und Kompetenzen:

Die Studierenden
- erklären wichtige kryptographische Verfahren und wenden diese praktisch an;
- nützen Software wie Maple, Python3 oder Sage zur Ver- und Entschlüsselung sowie zur Kryptoanalyse;
- erläutern wichtige zahlentheoretische Algorithmen, ihre theoretischen Hintergründe und ihre Funktion bei der Konstruktion von Public-Key-Kryptosystemen.

Literatur:

- Vorlesungsskript zum Modul
- J. Buchmann: Einführung in die Kryptographie
- J. Hoffstein, J. Pipher, J. H. Silvermann: An Introduction to Mathematical Cryptography

Verwendbarkeit des Moduls / Einpassung in den Musterstudienplan:

Das Modul ist im Kontext der folgenden Studienfächer/Vertiefungsrichtungen verwendbar:
[1] **Mathematik (1. Staatsprüfung für das Lehramt an Gymnasien)**
(Po-Vers. 2015w | NatFak | Mathematik (1. Staatsprüfung für das Lehramt an Gymnasien) | Module Fachwissenschaft Mathematik | Angewandte Mathematik)

Studien-/Prüfungsleistungen:

Modulabschlussprüfung: Angewandte Mathematik (Prüfungsnummer: 56021)
Untertitel: Kryptographie Lehramt Prüfungsleistung, Klausur, Dauer (in Minuten): 90
Anteil an der Berechnung der Modulnote: 100%
weitere Erläuterungen:
Klausur

Erstablegung: SS 2018, 1. Wdh.: WS 2018/2019

1. Prüfer: Wolfgang Ruppert

Organisatorisches:

Die Präsentation des Stoffes erfolgt in Vorlesungsform. Die weitere Aneignung der wesentlichen Begriffe und Techniken erfolgt durch wöchentliche Hausaufgaben.

Bemerkungen:

Wahlpflichtmodul in

- B. Sc. Mathematik, Technomathematik, Wirtschaftsmathematik und für das Lehramt vertieft