Dörte Haftendorn (Version 23.03.06)

Fachkompetenzen der angehenden Lehrerinnen und Lehrer
(Lehramt Gymnasien, BBS)

Teilbereich Zahlentheorie und Kryptografie

Elemente von Zahlentheorie und Algebra entwickeln und anwenden

Grundlegende Kompetenzen Zahlentheorie und Algebra:
Die angehenden Lehrerinnen und Lehrer sollen

- Grundlagen der Zahlentheorie(Teilbarkeit, ggT, kgV, Primzahlen...) kennen und dort Zusammenhänge begründen.
- den erweiterten Euklidischen Algorithmus (mit Vielfachsummendarstellung) begründen und sicher anwenden können.
- Primzahlsätze und Beweise -- insbeondere solche zur Teilbarkeit-- kennen.
- Restklassenringe als algebraische Stukturen kennen und in ihnen sicher rechnen.
- mit den primen Restklassen Gruppen vertraut sein, sie von Hand und auch mit Werkzeugen bestimmen, das Inverse der Elemente beschaffen, die Gruppenordnung auch als Wert der Euler-phi-Funktion kennen und bestimmen.
- Elementordnungen in endlichen Gruppen bestimmen, Nebenklassen aufstellen und beweisen, dass die Elementordnung Teiler der Gruppenordnung ist.
- der Eulerschen Satz für endliche Gruppen und den Kleinen Fermatschen Satz als seine Einschränkung auf prime Restklassengruppen kennen.

Grundlegende Kompetenzen Kryptografie
Die angehenden Lehrerinnen und Lehrer sollen

- das kryptographische RSA-Protokoll verstanden haben und vollständig von Hand (TR) mit kleinen Primzahlen durchziehen, seine Durchführbarkeit beweisen.
- dieses und mindestens ein weiteres kryptographisches Protokoll mit passenden Werkzeugen (CAS, o.a.) ausgehend vom zu verschlüsselden Text Schritt für Schritt erläutert mit großen Zahlen durchführen.
- für neu vorgelegte Protokolle die Durchführung verstehen, die Voraussetzungen nennen und die Durchführbarkeit beweisen.
- die fundamental neue Vorgehensweise der modernen Kryptografie von der bis dahin (1980) üblichen abgrenzen und dieses jeder Adressatengruppe angemessen erklären.

Weiterführende Kompetenzen
Die angehenden Lehrerinnen und Lehrer sollen

- Digitale Signatur mit den jeweiles behandelten krytografischen Protokollen durchführen und erklären können (auch von Hand mit kleinen Primzahlen).
- Public-Key-Protokolle, asymmetrische und symmetrische Protokolle, Schlüsseltausch, No-Key-Protokolle u.a. unterscheiden können und ihre Grundideen angemessen erklären.
- ein Protokoll für „Elektronisches Geld“ kennen, ggf. duchführen und beweisen
- verschiedene Primzahltests und ihre Zuverlässigkeit kennen.
- wissen, worauf die Sicherheit der modernen kryptografischen Verfahren beruht.
- Fragen zur Berechenbarkeit im Sinne der Informatik auf die Kryptografie beziehen.
- den Einsatz von Kryptografie in der Gesellschaft, Wirtschaft und Technik sinnvoll darstellen.