Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

t.MKR - Mathematik: Kryptologie

Kursverantwortung:	Samuel Beer, beer
verantwortliche OE:	
ECTS:	4
Schuljahr:	2012/2013
Zuletzt gespeichert:	22.01.2013 16:36

Fachkompetenz:

-

Methodenkompetenz:

-

Sozialkompetenz:

-

Selbstkompetenz:

-

Lernziel:

Kryptologische Methoden und deren mathematischen Grundlagen verstehen und anwenden können.
Kryptologische Algorithmen auf dem Computer implementieren und testen können.

Lerninhalt:

Algebraische Grundlagen (Gruppen, Ringe, Körper, modulare Arithmetik, Chinesischer Restsatz).
Über die Notwendigkeit grosser Primzahlen und wie sie erzeugt werden.
Primzahltests.
Public Key Systeme.
Faktorisierung ganzer Zahlen (quadratisches Sieb).
Bestimmen diskreter Logarithmen (Index calculus).
Einführung in elliptische Kurven.

Vorkenntnisse:

-

Durchführung:

Unterrichtsart	Anzahl Lektionen pro Woche
Vorlesung	14*2
Übung/Praktika	14*2
Blockunterricht	

Leistungsnachweise:

Laut Tabelle oder gemäss schriftlicher Festlegung des Dozierenden zu Semesterbeginn!

Bezeichnung	Art	Form	Umfang	Bewertung	Gewichtung
Leistungsnachweise während Unterrichtszeit					
Semesterendprüfung					

Unterrichtssprache:

Deutsch

Unterrichtsunterlagen:

Skript, Übungsserien

Ergänzende Literatur:

-

Bemerkungen:

-