Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

t.MKR - Mathematik: Kryptologie

Kursverantwortung:	Samuel Beer, beer
Credits:	4
Schuljahr:	2011/2012
Zuletzt gespeichert:	02.09.2011 09:35

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
Gruppenunterricht	
Blockunterricht	
Seminar	

Leistungsnachweise:

Laut Tabelle oder gemäss schriftlicher Festlegung des Dozierenden zu Semesterbeginn!

Anzahl	**Art**	**Gewichtung**
1	Modulendprüfung	60%
	Prüfungen während der Unterrichtszeit	
12	Übungsserien	Total 40%

Unterrichtssprache:

Deutsch

Unterrichtsunterlagen:

Skript, Übungsserien

Bemerkungen:

-