Zurich University of Applied Sciences

School of Engineering

t.MKR - Mathematik: Kryptologie

Person responsible for the course:	Samuel Beer, beer
Credits:	4
Valid for:	2011/2012
Last saved:	02.09.2011 09:35

Learning objectives:

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

Course content:

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.

Previous knowledge:

-

Teaching method:

Type of lesson:	Number of lessons per week:
Lecture	14*2
Tutorial/Practicum	14*2
Group teaching	
Block instruction	
Seminar	

Assessment:

According to the table or as specified in writing by the lecture at the beginning of the semester!

Number	Type	Weighting
1	End of term exam	60%
	Exam during the semester	
12	Exercises	40%

Language of instruction:

German

Instruction material:

Skript, Übungsserien

Comments:

-