COM-702 **Advanced Topics in Cryptology**

Lenstra Arjen

Cursus	Sem.	Type
Computer and Communication Sciences		Obl.
Mathematics		Obl.

Language of teaching	English
Credits	3
Session	
Exam	Oral presentation
Workload	90h
Hours	**42**
Courses	28
TP	14
Number of positions	

Frequency

Every 2 years

Remark

Next time: Fall 2019

Summary

discussion of recent cryptographic results on subjects that will be decided on during the first lectures. Possibilities include random number beacons, blockchains, or anything else that would be of interest to the students that want to practice studying and presenting crypto/math papers.

Content

In this course recent research in cryptology will be studied in an interactive fashion. Students will read, present, and discuss results from the most recent major cryptology conferences (such as Crypto and Eurocrypt) and may explore ways to improve those results. The course is intended to stimulate students in their own research.

Keywords

Cryptology; Algorithms; number theory

Learning Prerequisites

Recommended courses

General mathematics and elementary number theory background

Teaching methods

papers will be presented by the students and be discussed in detail.

Expected student activities

read papers, present them, participate in discussions

Assessment methods

assessment will be based on quality of presentations(s) and participation in class

Resources

Notes/Handbook

none