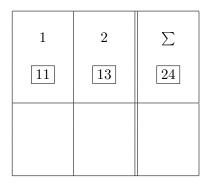
Name: _





Univ.-Prof. Dr. rer. nat. Rudolf Mathar, Univ.-Prof. Dr.-Ing. Anke Schmeink



Written examination

Advanced Methods of Cryptography

Monday, August 31, 2015, 08:30 a.m.

_____ Matr.-No.: ____

Field	d of study:			
Plea	ase pay attention to the following:			
1)	The exam consists of 2 problems . Please check the completeness of your copy. Only written solution these sheets will be considered. Removing the staples is not allowed.			
2)	The exam is passed with at least 25 points.			
3)	You are free in choosing the order of working on the problems. Your solution shall clearly show the approach and intermediate arguments.			
4)	Admitted materials: The sheets handed out with the exam and a non-programmable calculator.			
5)	Die Klausurergebnisse werden voraussichtlich am Freitag, den 11.09.2015, auf der Institutshomepage bekanntgegeben.			
	Die korrigierten Klausuren können am Montag, den 05.10.2015, um 13:00 Uhr im Seminarraum 333 des Lehrstuhls für Theoretische Informationstechnik, ICT cubes, Kopernikusstr. 16, eingesehen werden.			
Ackn	owledged: (Signature)			

Problem 1. (11 points)

a) Show that $\mathfrak{P} = \mathfrak{NP}$.

Problem 2. (13 points)

a) Show that the Riemann hypothesis holds.