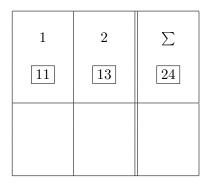
Name: \_



\_\_\_\_\_ Matr.-Nr.: \_\_\_\_



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



## Prüfungsklausur

## Advanced Methods of Cryptography

Montag, 31. August 2015, 08:30 Uhr

1)	Die Klausur besteht aus 2 Aufgaben. Bitte prüfen Sie die Vollständigkeit Ihres Exemplars nach.			
	Bei der Korrektur werden <b>nur</b> die Lösungen auf diesen Blättern berücksichtigt. Das Entfernen de Heftklammern ist <b>nicht</b> erlaubt.			
2)	Die Klausur ist mit mindestens 25 Punkten bestanden.			
3)	Die Reihenfolge der Bearbeitung der Aufgaben kann beliebig gewählt werden. Die Lösung der Aufgaben soll so erfolgen, dass der Lösungsweg deutlich erkennbar ist.			
4)	<b>Zugelassene Hilfsmittel:</b> Mit der Klausur ausgeteiltes Formelblatt, ein Lineal und ein gemäß der vora veröffentlichten Positivliste zugelassener Taschenrechner.			
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.			
Zur	Kenntnis genommen:			
	(Unterschrift)			

## Aufgabe 1. (11 Punkte)

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

## Aufgabe 2. (13 Punkte)

a) Show that the Riemann hypothesis holds.