Zahlentheorie und Kryptologie, Wintersemester 2012/13
M. Hortmann

Blatt 8

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen			**Gruppe**	**Tutor**
1	2	3	**Summe**	**bearbeitet**
5	5	5	10 Pkte=100%	

Entwerfen Sie kryptographische Protokolle für folgende Situationen

1. Roulette für eine Bank und mehrere Spieler.

2. Vor dem Protokolldurchlauf besitzt A 2 Bitstrings, welche B beide unbekannt sind.
Am Ende kennt B genau einen der beiden, aber A weiß nicht welchen.

3. Am Anfang besitzt A einen Bitstring, den B nicht kennt.
A und B einigen sich auf eine natürliche Zahl n.
Nach dem Protokolldurchlauf besitzt B mit der Wahrscheinlichkeit $1/n$ den Bitstring, aber A weiß nicht, ob B ihn dann kennt oder nicht. Falls B ihn nach Protokolldurchlauf nicht kennt, soll B auch keine Teilinformation über den String besitzen.

Bei der Darstellung der Lösungen sollen Sie genau beschreiben, wer wem in welcher Reihenfolge welche Nachrichten schickt, und dies soweit zum Verständnis nötig kommentieren. In den Protokollen sollen keine weiteren Parteien als die genannten eine Rolle spielen. Sie dürfen aber ggf. davon ausgehen, daß alle Beteiligten Teilnehmer eines Public Key Kryptosystems sind und daher insbesondere digitale Signaturen leisten und verifizieren können.

Womöglich müssen Sie bestimmte Arten von Betrugsversuchen "verbieten", bzw. Ehrlichkeit einer oder beider Parteien bei der Befolgung bestimmter oder gar aller Protokollschritte verlangen.