Sommersemester 2005

Hasso- Plattner- Institut, Universität Potsdam

Übung zur Vorlesung

Fachgebiet Internet- Technologien und - Systeme

Meinel / Kutzner

Aufgabenblatt 9
(NUR FÜR ULI-STUDENTEN)

(URL: http://www.hpi.uni- potsdam.de/index.php?id=411)

Abgabe: Mo, 20.06.2005, bis 12 Uhr MEZ (per E-Mail an mathias.kutzner@hpi.uni- potsdam.de)

Thema: Public- Key Krypto- Systeme

Erreichbare Punkte: 18

Aufgabe 1: **6 Punkte**

Verschlüsseln Sie die Nachricht „INFORMATION SECURITY“ mit dem RSA Verfahren. Verwenden Sie $n = 3337$ und $e = 79$.

Jeder Buchstabe wird laut der folgenden Tabelle als zweistellige Zahl repräsentiert. Der Klartext m setzt sich also durch die Aneinanderreihung der entsprechenden Zahlen zusammen.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20

U	V	W	X	Y	Z	
21	22	23	24	25	26	00

Teilen Sie Ihren Klartext in Blöcke von jeweils 4 Zeichen. Nehmen Sie die Verschlüsselung für jeden einzelnen Block vor. Geben Sie sowohl Ihren Rechenweg, als auch Ihre Chiffre- Blöcke an.

Aufgabe 2: **3 Punkte**

Berechnen Sie den zu Aufgabe 1 gehörenden privaten Schlüssel d. Erläutern Sie Ihre Vorgehensweise und geben Sie alle notwendigen Rechenschritte an.

Aufgabe 3: **9 Punkte**

Finden sie zwei unterschiedliche Primzahlen p und q, die beide genau 8 Bit für ihre Binärdarstellung benötigen. p und q sollen so gewählt werden, dass $n = p \cdot q$ binär dargestellt eine Länge von 16 Bit hat und n zusammen mit $e = 7395$ einen öffentlichen RSA- Schlüssel bildet. Ermitteln Sie zusätzlich den dazugehörigen privaten Schlüssel d.
Erläutern Sie ihre Überlegungen und geben Sie Ihren Rechenweg an.

Gibt es weitere Primzahlen p und q, die diese Bedingungen erfüllen? Wenn ja, geben Sie alle möglichen p, q, n und d an.