Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2010/2011
Übungsblatt 5

Abgabetermin: 08.12.2010 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikums Infrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungs Webseite zum Übungsberieb an.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email, in der Vorlesung oder vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 12: (H) Advanced Encryption Standard - Key Expansion

In Aufgabe 11 haben Sie sich mit dem Advanced Encryption Standard beschäftigt. Gegeben ist nun der folgende Schlüssel. Berechnen Sie den 1. Rundenschlüssel nach der ersten Key Expansion Phase.

Schlüssel: $\begin{pmatrix} 22 & 41 & B4 & 14 \\ 13 & 33 & A1 & 15 \\ 24 & 12 & 12 & 16 \\ 11 & 23 & F3 & 17 \end{pmatrix}$

Verwenden Sie für die Substitution die folgende S-Box:
S-BOX:

	0	1	2	3	4	5	6	7	8
0	0x00	0x10	0x20	0x01	0x18	0x19	0xB4	0x45	0x2C
1	0x01	0x25	0xE1	0xCB	0x10	0x13	0xA7	0x3B	0x1A
2	0x2D	0xA1	0x40	0x89	0x9D	0x34	0x12	0x5E	0x2D
3	0x38	0x40	0x2C	0x29	0x02	0x27	0xF1	0x01	0x89
4	0x43	0xF2	0x20	0x30	0x40	0x02	0xD8	0x7B	0x6A
5	0x3C	0x2A	0x28	0x34	0xA2	0x09	0x7F	0x4D	0xC2

Achten Sie darauf, dass Ihre Berechnung nachvollziehbar ist und geben Sie relevante Zwischenergebnisse an.

Aufgabe 13: (H) RSA und asymmetrische Verschlüsselung

a. Welche Probleme der symmetrischen Verschlüsselung löst die asymmetrische Verschlüsselung?

b. Welche Probleme der asymmetrischen Verschlüsselung löst die symmetrische Verschlüsselung?

c. Welche Probleme der symmetrischen und asymmetrischen Verschlüsselung löst eine Hybride Verschlüsselung

d. Bezogen auf die vorherige Teilaufgabe: Welche behält sie bei?

e. Erläutern Sie in Stichpunkten die Funktionsweise des RSA Verfahrens.

f. Die folgende Nachricht **68094034 128468343 143911297 122013244** wurde mit dem RSA-Verfahren mit den Parametern N=289648273 und e=17 verschlüsselt. Dabei wurde wie folgt vorgegangen: Der alphanumerische Klartext wurde zu Gruppen von je 3 Buchstaben zusammengefasst. Jeder solcher Dreiergruppen xyz, mit $x, y, z \in \{A, B, \ldots, Z\}$ wurde die Zahl $W(xyz) := w(x) \cdot 26^2 + w(y) \cdot 26 + w(z) \mod N$ zugeordnet, wobei $w : \{A, B, \ldots, Z\} \to \{0, 1, \ldots, 25\}$ jedem Buchstaben einen Wert anhand der Tabelle

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

zuordnet. $W(xyz) \in \mathbb{Z}/N\mathbb{Z}$ wurde dann mit RSA verschlüsselt. Wie lautet die Nachricht?

Aufgabe 14: (K) Schlüssellängen

a. Wie lange dauert es mit einem gegebenen Rechner (3GHz, ca. $3 * 10^6 \frac{\text{Schlüssel}}{\text{s}}$) einen symmetrischen Schlüssel der Länge 56 Bit / 128 Bit mittels Brute Force zu brechen?

b. Wie lange benötigt man, um mit der genannten Maschine einen 4096 Bit langes RSA Modul zu brechen?

c. Wie lange benötigt im Vergleich die Copacobana (20 Module ´a 120 FPGAs, $27.000.000 \frac{\text{Schlüssel}}{\text{s} * \text{FPGA}}$) für 56 Bit / 128 Bit lange DES Schlüssel?

d. Wie würde sich die Existenz eines DNA- oder Quantencomputers auf die Sicherheit von DES, AES und RSA auswirken?