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 4

Abgabetermin: 30.11.2010 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 10: (H) Kryptographisches System und DES

a. In der Vorlesung wurde das symmetrische Verschlüsselungsverfahren Data Encryption Standard (DES) erläutert. Welche Funktionen werden bei DES eingesetzt.

b. Welche Stärken bzw. Schwächen besitzt DES?

c. Ein Agent versucht einen Geheimtext zu entschlüsseln. Er weiß, dass zur Verschlüsselung folgende Tabelle benutzt wurde:

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

Weiter weiß er, dass zum Verschlüsseln eine Funktion $f : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}, x \mapsto ax + b$ verwendet wurde. Eine Häufigkeitsanalyse ergab, dass R und V die häufigsten Buchstaben im verschlüsselten Text sind (es wird angenommen, dass im Deutschen E und S die häufigsten Buchstaben sind). Entschlüsseln Sie die Nachricht: **IEFQRLRHQOBJQMRO**

Aufgabe 11: (H) Advanced Encryption Standard

Leiten Sie den Wert für das 1. Byte (1. Zeile, 1. Spalte) der Ausgabe des Rijndael-Algorithmus (Block-/Schlüsselgröße 128 Bit) am Ende der 1. Runde für die nachfolgenden Werte her. Beachten Sie, dass die Multiplikationen in GF(2^8) durchzuführen sind. Das zugehörige, irreduzible Polynom lautet $x^8 + x^4 + x^3 + x + 1$. **Benennen Sie die jeweilige Phase des AES-Algorithmus**, berechnen Sie die Werte und geben Sie die **alle** relevanten Zwischenergebnissen an, damit Ihr Rechenweg nachvollziehbar ist!

Klartext: $\begin{pmatrix} 11 & 33 & 33 & 44 \\ 22 & 22 & 44 & 11 \\ 33 & 44 & 11 & 22 \\ 44 & 11 & 22 & 33 \end{pmatrix}$ Schlüssel: $\begin{pmatrix} 02 & 40 & B4 & 04 \\ 03 & 30 & A1 & 05 \\ 04 & 10 & 12 & 06 \\ 01 & 20 & F3 & 07 \end{pmatrix}$

Spaltenmixmatrix: $\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$

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

In der ersten Key Expansion wurde folgender erster Rundenschlüssel berechnet:

1. Rundenschlüssel: $\begin{pmatrix} 1A & 5A & EE & 18 \\ B7 & 87 & 26 & B4 \\ 41 & 51 & 43 & 45 \\ 19 & 39 & CA & 18 \end{pmatrix}$