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 2008/2009
Übungsblatt 4

Abgabetermin: 19.11.2008 bis 14:00 Uhr

Achtung: Die schriftlichen Lösungen aller mit H gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben. Während des Semesters werden drei Übungsblätter korrigiert. Bei drei richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 8: (K) Steganographie

a. Betten Sie die Nachricht "*Dies ist eine versteckte Botschaft*" in die Bilder `rot.jpg`, `bunt.jpg` und `kariert.jpg`, welche Sie auf der Webseite herunterladen können ein. Verwenden Sie hierzu das Werkzeug *steghide*.

b. Extrahieren Sie die versteckten Nachrichten wieder aus den Bildern.

c. Vergleichen Sie die Histogramme der Bilder mit und ohne versteckter Nachricht. Was fällt auf?

d. Welche Techniken existieren, um Nachrichten in Bildern zu verstecken?

e. Wie robust sind die eingebetteten Nachrichten gegenüber nachträglichen Veränderungen am Bild?

Aufgabe 9: (H) Rijndael - AES

Berechnen Sie die ersten 4 Byte (1.Spalte) der Ausgabe des Rijndal Algorithmus (Block-/Schlüsselgröße 128 Bit) am Ende der ersten Runde für die nachfolgenden Werte! Geben Sie erforderliche Zwischenergebnisse an und achten Sie darauf, dass ihr Lösungsweg nachvollziehbar ist!

Klartext: $\begin{pmatrix} 01 & 05 & 09 & 0d \\ 02 & 06 & 0a & 0e \\ 03 & 07 & 0b & 0f \\ 04 & 08 & 0c & 10 \end{pmatrix}$ Schlüssel: $\begin{pmatrix} 11 & 55 & 99 & dd \\ 22 & 66 & aa & ee \\ 33 & 77 & bb & ff \\ 44 & 88 & cc & 00 \end{pmatrix}$

RCON(4) = 0x01000000 RCON(24) = 0x20000000
RCON(8) = 0x02000000 RCON(28) = 0x40000000
RCON(12) = 0x04000000 RCON(32) = 0x80000000
RCON(16) = 0x08000000 RCON(36) = 0x1B000000
RCON(20) = 0x10000000 RCON(40) = 0x36000000

S-BOX:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0x63	0x7c	0x77	0x7b	0xf2	0x6b	0x6f	0xc5	0x30	0x01	0x67	0x2b	0xfe	0xd7	0xab	0x76
1	0xca	0x82	0xc9	0x7d	0xfa	0x59	0x47	0xf0	0xad	0xd4	0xa2	0xaf	0x9c	0xa4	0x72	0xc0
2	0xb7	0xfd	0x93	0x26	0x36	0x3f	0xf7	0xcc	0x34	0xa5	0xe5	0xf1	0x71	0xd8	0x31	0x15
3	0x04	0xc7	0x23	0xc3	0x18	0x96	0x05	0x9a	0x07	0x12	0x80	0xe2	0xeb	0x27	0xb2	0x75
4	0x09	0x83	0x2c	0x1a	0x1b	0x6e	0x5a	0xa0	0x52	0x3b	0xd6	0xb3	0x29	0xe3	0x2f	0x84
5	0x53	0xd1	0x00	0xed	0x20	0xfc	0xb1	0x5b	0x6a	0xcb	0xbe	0x39	0x4a	0x4c	0x58	0xcf
6	0xd0	0xef	0xaa	0xfb	0x43	0x4d	0x33	0x85	0x45	0xf9	0x02	0x7f	0x50	0x3c	0x9f	0xa8
7	0x51	0xa3	0x40	0x8f	0x92	0x9d	0x38	0xf5	0xbc	0xb6	0xda	0x21	0x10	0xff	0xf3	0xd2
8	0xcd	0x0c	0x13	0xec	0x5f	0x97	0x44	0x17	0xc4	0xa7	0x7e	0x3d	0x64	0x5d	0x19	0x73
9	0x60	0x81	0x4f	0xdc	0x22	0x2a	0x90	0x88	0x46	0xee	0xb8	0x14	0xde	0x5e	0x0b	0xdb
A	0xe0	0x32	0x3a	0x0a	0x49	0x06	0x24	0x5c	0xc2	0xd3	0xac	0x62	0x91	0x95	0xe4	0x79
B	0xe7	0xc8	0x37	0x6d	0x8d	0xd5	0x4e	0xa9	0x6c	0x56	0xf4	0xea	0x65	0x7a	0xae	0x08
C	0xba	0x78	0x25	0x2e	0x1c	0xa6	0xb4	0xc6	0xe8	0xdd	0x74	0x1f	0x4b	0xbd	0x8b	0x8a
D	0x70	0x3e	0xb5	0x66	0x48	0x03	0xf6	0x0e	0x61	0x35	0x57	0xb9	0x86	0xc1	0x1d	0x9e
E	0xe1	0xf8	0x98	0x11	0x69	0xd9	0x8e	0x94	0x9b	0x1e	0x87	0xe9	0xce	0x55	0x28	0xdf
F	0x8c	0xa1	0x89	0x0d	0xbf	0xe6	0x42	0x68	0x41	0x99	0x2d	0x0f	0xb0	0x54	0xbb	0x16