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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2012/2013
Übungsblatt 6

Abgabetermin: 19.12.2012 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email an die Adresse **uebung-itsec_AT_lrz.de** oder schriftlich 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 13: (H) Advanced Encryption Standard - Key Expansion

Auf dem letzen Übungsblatt haben Sie sich mit dem Advanced Encryption Standard beschäftigt. Gegeben sei nun der folgende Schlüssel. Berechnen Sie den 1. Rundenschlüssel nach der ersten Key Expansion Phase.

Schlüssel: $\begin{pmatrix} 16 & 14 & C1 & 48 \\ 12 & 10 & B5 & 17 \\ 08 & 15 & 10 & 36 \\ 10 & 02 & A1 & 27 \end{pmatrix}$

Als Rundenkonstante RCON verwenden Sie:
RCON[1]: 0x01000000

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 14: (H) RSA

In der Vorlesung wurden symmetrische, asymmetrische und hybride Kryptosysteme im Detail erläutert. Der Algorithmus RSA wurde in PKCS#1 spezifiziert.

a. Wie ist in PKCS#1 der Wert des öffentlichen Schlüssels definiert. Was sagt dieser über die Wahl von e aus?

b. Welche Fehlermeldung wird gemäß Standard ausgegeben, wenn die Länge der chiffrierten Nachricht den Wert $n - 1$ übersteigt?

c. Gegeben seien zwei Primzahlen $p = 11$ und $q = 31$, sowie die ganzzahlige Klartext-Nachricht $m = 12$. Berechnen Sie den Chiffretext mithilfe des RSA-Verfahrens, verwenden Sie hierzu als Verschlüsselungsexponent $e = 17$. Achten Sie darauf, dass ihr Lösungsweg nachvollziehbar ist und überprüfen Sie Ihr Ergebnis durch entsprechendes Entschlüsseln.

d. Verschlüsseln Sie mit dem RSA-Verfahren den String *IT*. Die Ganzzahl-Codierung für Buchstaben laute $A = 01$. $B = 02$,...,$Z = 26$. Wählen Sie geeignete Primzahlen p und q, sodass Ihr RSA-Modul für die Verschlüsselung ausreichend groß ist. Berechnen Sie den Chiffretext, verwenden Sie hierzu für den Verschlüsselungsexponenten $e = 257$. Überprüfen Sie Ihre Berechnung durch eine anschließende Entschlüsselung.

e. Neben der Verschlüsselung kann das RSA-Verfahren auch zur Verifikation von Signaturen verwendet werden. Geben Sie die entsprechende Berechnungsvorschrift an, wenn s die Signatur, e und d die entsprechenden Schlüssel und n den RSA-Modul bezeichnen.

Aufgabe 15: (K) RSA - Chosen-Message-Attack

Aufgrund der Multiplikativität des RSA-Verfahrens ist dieser anfällig für eine Reihe von Angriffen. Eine Möglichkeit ist die so genannte *Chosen-Message-Attack*, bei der sich ein Angreifer eine beliebige Nachricht m signieren lassen kann.