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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2015/2016
Übungsblatt 8

Abgabetermin: 12.01.2016 bis 12:00 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 (über Uniworx als **Einzelabgabe**). Während des Semesters werden vier Übungsblätter ausgewählt, korrigiert und bewertet. Bei vier als korrekt bewerteten Lösungen (mind. 75% der erreichbaren Punkte) 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.

Bei Fragen zu Übungsaufgaben sowie generellen Anregungen, Verbesserungsvorschlägen, ... zum Übungsbetrieb wenden Sie sich bitte per Email an **`uebung-itsec@lrz.de`**.

Aufgabe 22: (H) Advanced Encryption Standard (AES) (10 Punkte)

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: $\begin{pmatrix} 17 & 21 & 03 & 06 \\ 08 & 43 & 24 & 16 \\ 33 & 12 & 41 & 23 \\ 51 & 37 & 11 & 35 \end{pmatrix}$ Schlüssel: $\begin{pmatrix} 11 & 22 & 33 & 44 \\ 2A & 33 & 44 & 11 \\ 32 & 44 & 11 & 22 \\ 44 & 11 & 22 & 33 \end{pmatrix}$

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	0xC4	0xA1	0x28	0x34	0xA2	0x09	0x7F	0x4D	0xC2
6	0x32	0x27	0x98	0x45	0x51	0x02	0xE4	0x89	0x2E
7	0xA6	0x2A	0x16	0x46	0x18	0x27	0xB3	0x1D	0xC8

In der ersten Key Expansion wurde folgender erster Rundenschlüssel berechnet:

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

Aufgabe 23: (H) Advanced Encryption Standard - Key Expansion (6 Punkte)

In der vorherigen Aufgabe 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 24: (H) Verschlüsselung und RSA (7 Punkte)

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

a. Welche Probleme der symmetrischen Verschlüsselung löst die asymmetrische Verschlüsselung? Welche hingegen nicht bzw. welchen gravierenden Nachteil weist sie auf?

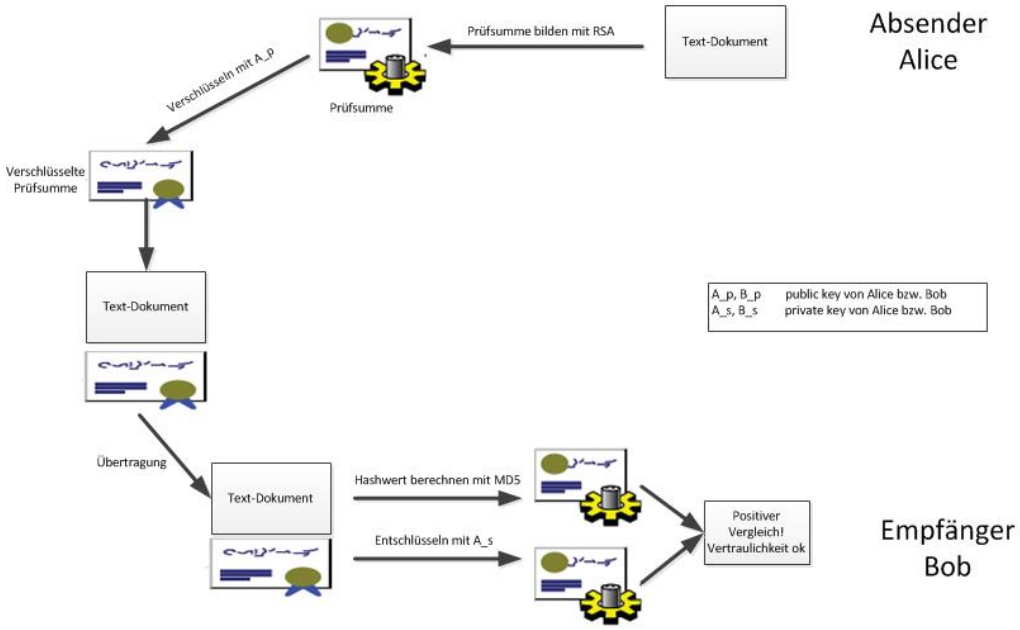

Abbildung 1: Fehlerhafter Ablauf einer digitalen Signatur

b. Wieviele Schlüssel benötigen Sie, wenn 10 Personen paarweise miteinander, abgesichert mithilfe eines symmetrischen Verschlüsselungsverfahrens kommunzieren wollen.

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 $A = 01$. $B = 02, \ldots, Z = 26$. 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. Abbildung 1 zeigt den generellen Ablauf für eine digitale Signatur, in dem jedoch mehrere Fehler enthalten sind. Finden und korrigieren Sie diese, damit die Signatur und deren Verifikation korrekt durchgeführt wird. Geben Sie auch an, welche(s) Sicherheitsziel(e) erreicht werden können und begründen Sie ihre Antwort kurz.