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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2021/2022
Übungsblatt 8

Besprechung: 11.01.2022 bis 12:00 Uhr

Aufgabe 31: (T) Advanced Encryption Standard (AES)

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: $\begin{pmatrix} 23 & 12 & 19 & 27 \\ 08 & 34 & 42 & 10 \\ 37 & 21 & 14 & 32 \\ 15 & 53 & 11 & 45 \end{pmatrix}$

0. Rundenschlüssel: $\begin{pmatrix} 12 & 07 & 1A & 33 \\ 30 & 01 & 16 & 54 \\ 14 & 63 & 27 & 11 \\ 44 & 23 & 55 & 10 \end{pmatrix}$

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

Verwenden Sie für ggf. durchzuführende Substitutionen folgende (fiktive) 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	0xB4	0x2C	0x29	0x02	0xA6	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, erste 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 32: (T) Verschlüsselung und RSA

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?

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. 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.

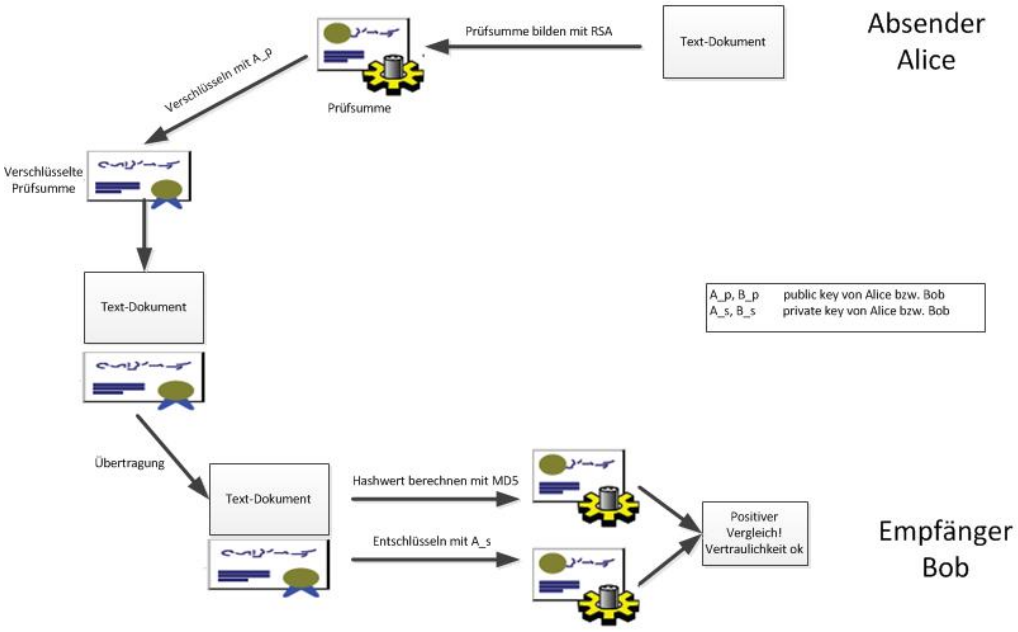

Abbildung 1: Fehlerhafter Ablauf einer digitalen Signatur