Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 04.12.2015
Abgabe: Mo. 14.12.2015 bis 14:00 (D3 Kasten)/14:45 Uhr (Fürstenallee)

Einführung in Kryptographie

WS 2015/2016

Heimübungszettel 4

AUFGABE 1 (8 Punkte)**:**
Bezeichne $\mathrm{DES}(m, k_1, k_2, \ldots, k_{16})$ den Chiffretext bei DES-Verschlüsselung eines Klartextes m mit den Rundenschlüsseln $k_1, k_2, \ldots, k_{16}$. Für eine Bitfolge $w \in \{0,1\}^*$ bezeichne $\overline{w}$ das Komplement von w, d.h., die Bitfolge die aus w entsteht, indem jede 1 durch eine 0 und jede 0 durch eine 1 ersetzt wird.
Sei $c = \mathrm{DES}(m, k_1, k_2, \ldots, k_{16})$. Zeigen Sie, dass dann $\overline{c} = \mathrm{DES}(\overline{m}, \overline{k}_1, \overline{k}_2, \ldots, \overline{k}_{16})$ gilt.

AUFGABE 2 (6 Punkte)**:**
Betrachten Sie den internen Zustand von AES bestehend aus 16 bytes als Element des Vektorraums $\mathbb{F}_{256}^{4\times 4}$. Welche der in AES verwendeten Funktionen *SubBytes*, *ShiftRows*, *MixColumns* und *AddRoundKey* sind affin-linear als Operation auf dem Vektorraum $\mathbb{F}_{256}^{4\times 4}$ und welche nicht? Beweisen Sie die Linearität oder geben Sie Gegenbeispiele an.

AUFGABE 3 (8 Punkte)**:**
Welche Auswirkungen haben die folgenden Modifikationen auf die Sicherheit von AES?

a) Sie erweitern die letzte Runde, so dass sie sich nun *nicht* mehr von den $r-1$ vorausgegangenen Runden unterscheidet. D.h., auch die letzte Runde besteht aus den Operationen AddRoundKey, SubBytes, ShiftRows und MixColumns.

b) Sie entfernen die Operation SubBytes aus AES. D.h., eine Verschlüsselung besteht nur noch aus der wiederholten Anwendung der Operationen AddRoundKey, ShiftRows und MixColumns.

c) Sie entfernen die Operation ShiftRows aus AES. D.h., eine Verschlüsselung besteht nur noch aus der wiederholten Anwendung der Operationen AddRoundKey, SubBytes und MixColumns.

d) Sie entfernen die Operation MixColumns aus AES. D.h., eine Verschlüsselung besteht nur noch aus der wiederholten Anwendung der Operationen AddRoundKey, SubBytes und ShiftRows.

AUFGABE 4 (8 Punkte)**:**
Sei $N = 33$ ein RSA-Modul.

a) Welche der beiden Tupel $(N, 5)$ und $(N, 9)$ sind gültige öffentliche Schlüssel?

b) Bestimmen Sie den geheimen Exponenten d zum öffentlichen Exponenten $e = 7$.

c) Welche weiteren Möglichkeiten für den öffentlichen Exponenten existieren unter dem gegebenem RSA-Modul N zusätzlich zu $e = 7$?

d) Entschlüsseln Sie den Chiffretext $c = 4$ mit dem geheimen Schlüssel aus Teilaufgabe b).