Übungen zur Kryptologie 1 Sommersemester 2002
Johannes Köbler/Olaf Beyersdorff

Übungsblatt 12

Aufgabe 41

Der „normale“ Ablauf einer Entschlüsselung beim AES erfolgt nach folgendem Schema:

AddRoundKey(K^{10})
ShiftRows^{-1}
SubBytes^{-1}
`for i:= 9 downto 1 do`
  AddRoundKey(K^i)
  MixColumns^{-1}
  ShiftRows^{-1}
  SubBytes^{-1}
`end`
AddRoundKey(K^0)

Zeigen Sie, dass alternativ auch dieselbe Reihenfolge der Operationen wie bei der Verschlüsselung benutzt werden kann.

Aufgabe 42 (schriftlich, 10 Punkte)

a) Zeigen Sie, dass für jedes $a \in \mathbb{Z}_m^*$ ein $k > 0$ existiert mit $a^k \equiv 1 \pmod{m}$.

b) Sei nun $\mathrm{ord}_m(a) = k$. Zeigen Sie, dass die Menge

$$\{a^0 \bmod m, a^1 \bmod m, a^2 \bmod m, \ldots\}$$

eine Untergruppe von $\mathbb{Z}_m^*$ mit genau k Elementen bildet. Folgern Sie $k|\varphi(m)$.

c) Zeigen Sie $a^i \equiv_m a^j$ genau dann, wenn $i \equiv_{\mathrm{ord}_m(a)} j$.

Aufgabe 43

Berechnen Sie $\varphi(75\,600)$, $\varphi(14\,948)$, $\log_{7,3} 4$, $\log_{37,2} 3$, $\mathrm{ord}_7(2)$ und $\mathrm{ord}_{31}(2)$.

Aufgabe 44

Seien $m_1, \ldots, m_{n+1} \in \mathbb{N}$. Sei $g_i = \mathrm{ggT}(m_i, m_{n+1})$, $i = 1, \ldots, n$. Zeigen Sie

$$\mathrm{kgV}(g_1, \ldots, g_n) = \mathrm{ggT}(\mathrm{kgV}(m_1, \ldots, m_n), m_{n+1}).$$