Datensicherheit, Übung 8

Henry Haustein

Aufgabe 1

(a) Insgesamt 10 Runden $\Rightarrow$ 11 Rundenschlüssel

(b) Jeder Schlüssel besteht aus 4 w's $\Rightarrow$ 44 w's

(c) Rcon[2] = [x^1, 00, 00, 00] = [02, 00, 00, 00] wird für w_8 bis w_{11} gebraucht;
Rcon[3] = [x^2, 00, 00, 00] = [04, 00, 00, 00] für w_{12} bis w_{15}

Aufgabe 2

k_0 = AB 8F 20 D3 74 E9 5C 37 32 C8 52 30 1F C6 7F 3E
$w_4 = SubWord(Rot(w_3)) \oplus Rcon[1] \oplus w_0 = SubWord([C6, 7F, 3E, 1F]) \oplus [01, 00, 00, 00] = [B4, D2, B2, C0] \oplus$
$[01, 00, 00, 00] \oplus [AB, 8F, 20, D3] = [B5, D2, B2, C0] \oplus [AB, 8F, 20, D3] = [1E, 5D, 92, 13]$
$w_5 = w_4 \oplus w_1 = [1E, 5D, 92, 13] \oplus [74, E9, 5C, 37] = [6A, B4, CE, 24]$
$w_6 = w_5 \oplus w_2 = [6A, B4, CE, 24] \oplus [32, C8, 52, 30] = [58, 7C, 9C, 14]$
$w_7 = w_6 \oplus w_3 = [58, 7C, 9C, 14] \oplus [1F, C6, 7F, 3E] = [47, BA, E3, 2A]$

Aufgabe 3

letzte Runde: Shift^{-1}, Sub^{-1} vertauschen
vorletzte Runden: $\oplus k_{r-1}$, MC^{-1} vertauschen ($k_{r-1} \rightarrow k'_{r-1}$) und Shift^{-1}, Sub^{-1} vertauschen, ...
$\Rightarrow$ neue Reihenfolge: Sub^{-1}, Shift^{-1}, MC^{-1}, $\oplus k'_{r-1}$, Sub^{-1}, Shift^{-1}, ... $\Rightarrow$ selbe Reihenfolge wie bei der Verschlüsselung

Aufgabe 4

Bis $j = i - 1$ kann alles korrekt entschlüsselt werden. Da c_i fehlt, entschlüsselt der Empfänger $m_i = dec(k, c_{c+1}) \oplus c_{i-1}$, was schief geht. Dann $m_{i+1} = dec(k, c_{i+1}) \oplus c_{i-1}$, was fehlerhaft ist. Ab $m_{i+2} = dec(k, c_{i+2}) \oplus c_{i+1}$ geht wieder alles.

Aufgabe 5

Original: $c_{i+1} = enc(k, (m_{i+1} \oplus c_i))$
Überprüfen: $c'_{i+1} = enc(k, (m' \oplus c_i))$
$c'_{i+2} = enc(k, (m_{i+1} \oplus c'_{i+1}))$ $\Rightarrow$ Fehlerfortpflanzung

Aufgabe 6

ECB: parallelisierbar, CBC: nicht parallelisierbar in enc(), parallelisierbar in dec(), CTR: parallelisierbar