Kryptografie und -analyse, Übung 4

Henry Haustein

Aufgabe 1: DES

(a) Ergebnis der Expansionsabbildung: 110110|100110
$\oplus$ Schlüssel: 000010|111100
1. Block in $S1_0$: 0100
2. Block in $S2_3$: 0010

(b) Wenn die Register C und D immer gleich sind, so ist der Rundenschlüssel immer gleich. Damit sind Ver- und Entschlüsselung identisch.

(c) Es gilt

m	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8
P					m_6	m_7	m_4	m_5
$\oplus k$					k_0	k_1	k_2	k_3
$\oplus L_0$					m_1	m_2	m_3	m_4
c	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8

$\Rightarrow k_0 = m_0 \oplus m_6 \oplus c_4 = 1$
$\Rightarrow k_1 = m_1 \oplus m_7 \oplus c_5 = 0$
$\Rightarrow k_2 = m_2 \oplus m_4 \oplus c_6 = 0$
$\Rightarrow k_3 = m_3 \oplus m_5 \oplus c_7 = 1$

(d) Meet-in-the-middle-Angriff, zweifache Verschlüsselung (Aufwand $2^{56} \cdot 2^{56} = 2^{112}$) und einfache Entschlüsselung (Aufwand 2^{56})

Differentielle Kryptoanalyse

(a) $S1_I^* = S1_I \oplus S1_I' = 110110 \oplus 011011 = 101101$
$S1_O = S1_2(110110) = 0111$, $S1_O^* = S1_3(101101) = 0001$
$S1_O' = 0111 \oplus 0001 = 0110$

(b) $S1_E' = 010001 \oplus 010010 = 000011$. Von den 64 möglichen Inputpaaren brauchen wir diejenigen, die Inputdifferenz von 3_{16} und Outputdifferenz 9_{16} haben. Dazu schauen wir in der Verteilungstabelle in der Spalte 9 nach Einsen. Es gibt 4 Inputpaare: (4,7), (7,4), (31,32), (32,31).
$S1_K = S1_I \oplus S1_E$

$S1_I$, $S1_I^*$	Schlüsselkandidaten
4, 7	15, 16
31, 32	20, 23

⇒ gesuchter Schlüssel ist 23
⇒ Differenz zwischen den Schlüsselkandidaten ist die Inputdifferenz der Eingaben. Mit immer derselben Differenz ist es nicht möglich einen eindeutigen Schlüssel zu erhalten.