Übungen zur Kryptologie 1 Sommersemester 2002
Johannes Köbler/Olaf Beyersdorff

Übungsblatt 10

Aufgabe 35

a) Wir betrachten das SPN aus der Vorlesung, wobei die S-Box $\pi_{S''}$ mit

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_{S'}(z)$	E	2	1	3	D	9	0	6	F	4	5	A	8	C	7	B

benutzt wird. Bestimmen Sie die Werte $D(a,b)$ für $a,b \in \{0,1\}^4$.

b) Finden Sie geeignete Differentiale für die vier S-Boxen S_1^1, S_4^1, S_4^2 und S_4^3, um eine Differentialspur mit einem Weitergabequotienten von $^{27}/_{2048}$ zu bilden.

Aufgabe 36

Schreiben Sie ein Programm, das den in der vorigen Aufgabe skizzierten Angriff auf ein SPN mittels differentieller Kryptoanalyse ausführt. Testen Sie Ihr Programm mit zufällig generierten Klartext-Kryptotext-Doppelpaaren, um die Anzahl t der zur Bestimmung des korrekten Subkey benötigten Doppelpaare herauszufinden.

Aufgabe 37 (schriftlich, 10 Punkte)

a) Zeigen Sie, dass der Kryptotext einer Feistel-Chiffre dadurch entschlüsselt werden kann, dass man ihn nochmals verschlüsselt, wobei die Rundenschlüssel in der umgekehrten Reihenfolge benutzt werden.

b) Beweisen Sie, dass die vier Schlüssel (in Hexadezimaldarstellung)

```
0101010101010101, FEFEFEFEFEFEFEFE,
1F1F1F1F0E0E0E0E, E0E0E0E0F1F1F1F1
```

die einzigen schwachen Schlüssel für den DES-Algorithmus sind.

c) Begründen Sie, dass für schwache Schlüssel K gilt:

$$\mathrm{DES}(K, \mathrm{DES}(K, x)) = x.$$

(Hinweis: Verwenden Sie Teilaufgabe a).

d) Ein DES-Schlüssel K heißt semi-schwach, falls er genau zwei verschiedene Rundenschlüssel erzeugt (d.h. falls gilt $\|\{K^1,\ldots, K^{16}\}\|=2$). Geben Sie zwei semi-schwache Schlüssel K und K' an mit

$$\mathrm{DES}(K', \mathrm{DES}(K, x)) = x.$$