

Aufgabe 17

- (a) Zwecks Übersichtlichkeit wurde im Folgenden Pasch durch 'P' und Nicht-Pasch durch 'NP' ersetzt.

$$\mathcal{P}[P, 2] = \frac{1}{36}, \mathcal{P}[P|2] = \frac{\mathcal{P}[P,2]}{\mathcal{P}[2]} = \frac{\frac{1}{36}}{\frac{1}{36}} = 1, \mathcal{P}[2|P] = \frac{\mathcal{P}[2,P]}{\mathcal{P}[P]} = \frac{\frac{1}{36}}{\frac{1}{6}} = \frac{1}{6}$$

$$\mathcal{P}[NP, 2] = 0, \mathcal{P}[NP|2] = \frac{\mathcal{P}[NP,2]}{\mathcal{P}[2]} = \frac{0}{\frac{1}{36}} = 0, \mathcal{P}[2|NP] = \frac{\mathcal{P}[2,NP]}{\mathcal{P}[NP]} = \frac{0}{\frac{5}{6}} = 0$$

$$\mathcal{P}[P, 3] = 0, \mathcal{P}[P|3] = \frac{\mathcal{P}[P,3]}{\mathcal{P}[3]} = \frac{0}{\frac{1}{18}} = 0, \mathcal{P}[3|P] = \frac{\mathcal{P}[3,P]}{\mathcal{P}[P]} = \frac{0}{\frac{1}{6}} = 0$$

$$\mathcal{P}[NP, 3] = \frac{1}{18}, \mathcal{P}[NP|3] = \frac{\mathcal{P}[NP,3]}{\mathcal{P}[3]} = \frac{\frac{1}{18}}{\frac{1}{18}} = 1, \mathcal{P}[3|NP] = \frac{\mathcal{P}[3,NP]}{\mathcal{P}[NP]} = \frac{\frac{1}{18}}{\frac{1}{6}} = \frac{1}{3}$$

$$\mathcal{P}[P, 4] = \frac{1}{36}, \mathcal{P}[P|4] = \frac{\mathcal{P}[P,4]}{\mathcal{P}[4]} = \frac{\frac{1}{36}}{\frac{1}{12}} = \frac{1}{3}, \mathcal{P}[4|P] = \frac{\mathcal{P}[4,P]}{\mathcal{P}[P]} = \frac{\frac{1}{36}}{\frac{1}{6}} = \frac{1}{6}$$

$$\mathcal{P}[NP, 4] = \frac{1}{18}, \mathcal{P}[NP|4] = \frac{\mathcal{P}[NP,4]}{\mathcal{P}[4]} = \frac{\frac{1}{18}}{\frac{1}{12}} = \frac{2}{3}, \mathcal{P}[4|NP] = \frac{\mathcal{P}[4,NP]}{\mathcal{P}[NP]} = \frac{\frac{1}{18}}{\frac{1}{6}} = \frac{1}{3}$$

$$\mathcal{P}[P, 5] = 0, \mathcal{P}[P|5] = \frac{\mathcal{P}[P,5]}{\mathcal{P}[5]} = \frac{0}{\frac{1}{9}} = 0, \mathcal{P}[5|P] = \frac{\mathcal{P}[5,P]}{\mathcal{P}[P]} = \frac{0}{\frac{1}{6}} = 0$$

$$\mathcal{P}[NP, 5] = \frac{1}{9}, \mathcal{P}[NP|5] = \frac{\mathcal{P}[NP,5]}{\mathcal{P}[5]} = \frac{\frac{1}{9}}{\frac{1}{9}} = 1, \mathcal{P}[5|NP] = \frac{\mathcal{P}[5,NP]}{\mathcal{P}[NP]} = \frac{\frac{1}{9}}{\frac{2}{15}} = \frac{5}{6}$$

$$\mathcal{P}[P, 6] = \frac{1}{36}, \mathcal{P}[P|6] = \frac{\mathcal{P}[P,6]}{\mathcal{P}[6]} = \frac{\frac{1}{36}}{\frac{5}{36}} = \frac{1}{5}, \mathcal{P}[6|P] = \frac{\mathcal{P}[6,P]}{\mathcal{P}[P]} = \frac{\frac{1}{36}}{\frac{1}{6}} = \frac{1}{6}$$

$$\mathcal{P}[NP, 6] = \frac{1}{9}, \mathcal{P}[NP|6] = \frac{\mathcal{P}[NP,6]}{\mathcal{P}[6]} = \frac{\frac{1}{9}}{\frac{5}{36}} = \frac{4}{5}, \mathcal{P}[6|NP] = \frac{\mathcal{P}[6,NP]}{\mathcal{P}[NP]} = \frac{\frac{1}{9}}{\frac{2}{15}} = \frac{5}{6}$$

$$\mathcal{P}[P, 7] = 0, \mathcal{P}[P|7] = \frac{\mathcal{P}[P,7]}{\mathcal{P}[7]} = \frac{0}{\frac{1}{6}} = 0, \mathcal{P}[7|P] = \frac{\mathcal{P}[7,P]}{\mathcal{P}[P]} = \frac{0}{\frac{1}{6}} = 0$$

$$\mathcal{P}[NP, 7] = \frac{1}{6}, \mathcal{P}[NP|7] = \frac{\mathcal{P}[NP,7]}{\mathcal{P}[7]} = \frac{\frac{1}{6}}{\frac{1}{6}} = 1, \mathcal{P}[7|NP] = \frac{\mathcal{P}[7,NP]}{\mathcal{P}[NP]} = \frac{\frac{1}{6}}{\frac{1}{5}} = \frac{5}{6}$$

$$\mathcal{P}[P, 8] = \frac{1}{36}, \mathcal{P}[P|8] = \frac{\mathcal{P}[P,8]}{\mathcal{P}[8]} = \frac{\frac{1}{36}}{\frac{5}{36}} = \frac{1}{5}, \mathcal{P}[8|P] = \frac{\mathcal{P}[8,P]}{\mathcal{P}[P]} = \frac{\frac{1}{36}}{\frac{1}{6}} = \frac{1}{6}$$

$$\mathcal{P}[NP, 8] = \frac{1}{9}, \mathcal{P}[NP|8] = \frac{\mathcal{P}[NP,8]}{\mathcal{P}[8]} = \frac{\frac{1}{9}}{\frac{5}{36}} = \frac{4}{5}, \mathcal{P}[8|NP] = \frac{\mathcal{P}[8,NP]}{\mathcal{P}[NP]} = \frac{\frac{1}{9}}{\frac{2}{15}} = \frac{5}{6}$$

$$\mathcal{P}[P, 9] = 0, \mathcal{P}[P|9] = \frac{\mathcal{P}[P,9]}{\mathcal{P}[9]} = \frac{0}{\frac{1}{9}} = 0, \mathcal{P}[9|P] = \frac{\mathcal{P}[9,P]}{\mathcal{P}[P]} = \frac{0}{\frac{1}{6}} = 0$$

$$\mathcal{P}[NP, 9] = \frac{1}{9}, \mathcal{P}[NP|9] = \frac{\mathcal{P}[NP,9]}{\mathcal{P}[9]} = \frac{\frac{1}{9}}{\frac{1}{9}} = 1, \mathcal{P}[9|NP] = \frac{\mathcal{P}[9,NP]}{\mathcal{P}[NP]} = \frac{\frac{1}{9}}{\frac{2}{15}} = \frac{5}{6}$$

$$\mathcal{P}[P, 10] = \frac{1}{36}, \mathcal{P}[P|10] = \frac{\mathcal{P}[P,10]}{\mathcal{P}[10]} = \frac{\frac{1}{36}}{\frac{1}{12}} = \frac{1}{3}, \mathcal{P}[10|P] = \frac{\mathcal{P}[10,P]}{\mathcal{P}[P]} = \frac{\frac{1}{36}}{\frac{1}{6}} = \frac{1}{6}$$

$$\mathcal{P}[NP, 10] = \frac{1}{18}, \mathcal{P}[NP|10] = \frac{\mathcal{P}[NP,10]}{\mathcal{P}[10]} = \frac{\frac{1}{18}}{\frac{1}{12}} = \frac{2}{3}, \mathcal{P}[10|NP] = \frac{\mathcal{P}[10,NP]}{\mathcal{P}[NP]} =$$

$$\frac{\frac{1}{18}}{\frac{1}{6}} = \frac{1}{3}$$

$$\mathcal{P}[P, 11] = 0, \mathcal{P}[P|11] = \frac{\mathcal{P}[P,11]}{\mathcal{P}[11]} = \frac{0}{\frac{1}{18}} = 0, \mathcal{P}[11|P] = \frac{\mathcal{P}[11,P]}{\mathcal{P}[P]} = \frac{0}{\frac{1}{6}} = 0$$

$$\mathcal{P}[NP, 11] = \frac{1}{18}, \mathcal{P}[NP|11] = \frac{\mathcal{P}[NP,11]}{\mathcal{P}[11]} = \frac{\frac{1}{18}}{\frac{1}{18}} = 1, \mathcal{P}[11|NP] = \frac{\mathcal{P}[11,NP]}{\mathcal{P}[NP]} =$$

$$\frac{\frac{1}{18}}{\frac{1}{6}} = \frac{1}{3}$$

$$\mathcal{P}[P, 12] = \frac{1}{36}, \mathcal{P}[P|12] = \frac{\mathcal{P}[P,12]}{\mathcal{P}[12]} = \frac{\frac{1}{36}}{\frac{1}{36}} = 1, \mathcal{P}[12|P] = \frac{\mathcal{P}[12,P]}{\mathcal{P}[P]} = \frac{\frac{1}{36}}{\frac{1}{6}} =$$

$$\frac{1}{6}, \mathcal{P}[NP, 12] = 0, \mathcal{P}[NP|12] = \frac{\mathcal{P}[NP,12]}{\mathcal{P}[12]} = \frac{0}{\frac{1}{36}} = 0, \mathcal{P}[12|NP] = \frac{\mathcal{P}[12,NP]}{\mathcal{P}[NP]} =$$

$$\frac{0}{\frac{5}{6}} = 0$$

Diese Auflistung wurde mittels

`./uebung5.pl prob17a > aufgabe17a.tex`

ermittelt, welches einfach alle werfbaren Würfe ausprobiert.

- (b) Genau dann wenn $(\mathcal{X}_1 \otimes \mathcal{X}_2)$ und $(\mathcal{X}_2 \otimes \mathcal{X}_3)$ unabhängig sind gilt das Piling-Up-Lemma. Daraus folgt betrachtet man $\mathcal{X}_1 \otimes \mathcal{X}_3 = (\mathcal{X}_1 \otimes \mathcal{X}_2) \otimes (\mathcal{X}_1 \otimes \mathcal{X}_3)$

muss gelten $\epsilon_{1,3} = 2 \cdot \epsilon_{1,2} \cdot \epsilon_{2,3}$.
 Dies sowohl für $\epsilon_1 = 0 \wedge \epsilon_3 = 0$.

$$\begin{aligned}\epsilon_{1,2} &= 0 \\ \epsilon_{1,3} &= 0 \\ \epsilon_{2,3} &= 0\end{aligned}$$

Als auch für $|\epsilon_2| = \frac{1}{2}$

$$\begin{aligned}\epsilon_{1,2} &= 2 \cdot \epsilon_1 \cdot \frac{1}{2} = \epsilon_1 \\ \epsilon_{1,3} &= 2 \cdot \epsilon_1 \cdot \epsilon_3 \\ \epsilon_{2,3} &= 2 \cdot \frac{1}{2} \cdot \epsilon_3 = \epsilon_3\end{aligned}$$

bzw.

$$\begin{aligned}\epsilon_{1,2} &= 2 \cdot \epsilon_1 \cdot -\frac{1}{2} = -\epsilon_1 \\ \epsilon_{1,3} &= 2 \cdot \epsilon_1 \cdot \epsilon_3 \\ \epsilon_{2,3} &= 2 \cdot -\frac{1}{2} \cdot \epsilon_3 = -\epsilon_3\end{aligned}$$

der Fall.

Andererseits gelte $\epsilon_1 \neq 0 \wedge \epsilon_3 \neq 0 \wedge |\epsilon_3| \neq \frac{1}{2}$

$$\begin{aligned}\epsilon_{1,2} &= 2 \cdot \epsilon_1 \cdot \epsilon_2 \\ \epsilon_{1,3} &= 2 \cdot \epsilon_1 \cdot \epsilon_3 \\ \epsilon_{2,3} &= 2 \cdot \epsilon_2 \cdot \epsilon_3 \\ \Rightarrow 0 &\leq |2 \cdot \epsilon_1 \cdot \epsilon_2| < |\epsilon_1| \wedge 0 \leq |2 \cdot \epsilon_2 \cdot \epsilon_3| < |\epsilon_3| \wedge 0 < |2 \cdot \epsilon_1 \cdot \epsilon_3| \\ \Rightarrow 0 &\leq 2 \cdot \underbrace{|2 \cdot \epsilon_1 \cdot \epsilon_2|}_{<|\epsilon_1|} \cdot \underbrace{|2 \cdot \epsilon_2 \cdot \epsilon_3|}_{<|\epsilon_3|} < |2 \cdot \epsilon_1 \cdot \epsilon_3| \\ \Rightarrow 8 \cdot \epsilon_1 \cdot \epsilon_2^2 \cdot \epsilon_3 &\neq 2 \cdot \epsilon_1 \cdot \epsilon_3\end{aligned}$$

(c)

$$\begin{aligned}
\text{SBox 1 } \epsilon_{\mathcal{X}_2 \otimes \mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \mathcal{Y}_3 \otimes \mathcal{Y}_4} &= \frac{-9}{32} \\
\text{SBox 2 } \epsilon_{\mathcal{X}_2 \otimes \mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \mathcal{Y}_3 \otimes \mathcal{Y}_4} &= \frac{-3}{16} \\
\text{SBox 3 } \epsilon_{\mathcal{X}_2 \otimes \mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \mathcal{Y}_3 \otimes \mathcal{Y}_4} &= \frac{5}{32} \\
\text{SBox 4 } \epsilon_{\mathcal{X}_2 \otimes \mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \mathcal{Y}_3 \otimes \mathcal{Y}_4} &= \frac{1}{8} \\
\text{SBox 5 } \epsilon_{\mathcal{X}_2 \otimes \mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \mathcal{Y}_3 \otimes \mathcal{Y}_4} &= \frac{-5}{16} \\
\text{SBox 6 } \epsilon_{\mathcal{X}_2 \otimes \mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \mathcal{Y}_3 \otimes \mathcal{Y}_4} &= \frac{11}{64} \\
\text{SBox 7 } \epsilon_{\mathcal{X}_2 \otimes \mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \mathcal{Y}_3 \otimes \mathcal{Y}_4} &= \frac{-7}{32} \\
\text{SBox 8 } \epsilon_{\mathcal{X}_2 \otimes \mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \mathcal{Y}_3 \otimes \mathcal{Y}_4} &= \frac{-1}{4}
\end{aligned}$$

Diese Ergebnisse wurden mittels

```
./uebung5.pl prob17c
```

ermittelt, welches wie im Skript auf Seite 41 zunächst eine vollständige Tabelle aufstellt und darin dann jeweils die Anzahl der Zeilen ermittelt, für die die Zufallsvariable 0 annimmt; daraus ergibt sich dann p_i , wodurch dann das Bias $\epsilon_i = p_i - \frac{1}{2}$ gegeben ist.

Aufgabe 18

S-Box	Zufallsvariable	Bias
S_4^1	$\mathcal{T}_1 = \mathcal{U}_{16}^1 \otimes \mathcal{V}_{13}^1$	$-\frac{1}{4}$
S_1^2	$\mathcal{T}_2 = \mathcal{U}_4^2 \otimes \mathcal{V}_1^2$	$-\frac{1}{4}$
S_1^3	$\mathcal{T}_3 = \mathcal{U}_1^3 \otimes \mathcal{V}_1^3 \otimes \mathcal{V}_3^3$	$-\frac{1}{4}$

(a)

Die S-Boxen S_4^1, S_1^2, S_1^3 scheinen hier eine gute Wahl; $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3$ werden geschickt so gewählt, dass beim Auflösen ein Term mit \mathcal{X}_{16} und \mathcal{U}_1^4 sowie \mathcal{U}_9^4 sowie einigen weiteren Key-Bits herauskommt; der Bias von $\mathcal{T}_1 \otimes \mathcal{T}_2 \otimes \mathcal{T}_3$ ist dann der Gesuchte. Die Biase der S-Boxen wurden mittels der N_L -Wertetabelle von π'_S ermittelt, welche durch Aufruf von

```
./uebung5.pl nl
./uebung5.pl prob18a
```

ermittelt wurden; Genauer gilt ja $\epsilon(a, b) = \frac{N_L(a, b) - 8}{16}$; hier sind (a, b) jeweils $(1, 8), (1, 8), (8, 10)$ und $N_L(a, b)$ jeweils $4, 4, 4$ und damit die Biase $-\frac{1}{4}, -\frac{1}{4}, -\frac{1}{4}$. Somit ist $\epsilon_{\mathcal{T}_1 \otimes \mathcal{T}_2 \otimes \mathcal{T}_3} = 2^2 \cdot -\frac{1}{4} \cdot -\frac{1}{4} \cdot -\frac{1}{4} = -\frac{1}{16}$ nach Piling-Up

Lemma. Dass dies auch das Bias von $\mathcal{X}_{16} \otimes \mathcal{U}_1^4 \otimes \mathcal{U}_4^9$ ist, lässt sich durch Auflösung von $\mathcal{T}_1 \otimes \mathcal{T}_2 \otimes \mathcal{T}_3$ zeigen :

$$\begin{aligned}
 \mathcal{T}_1 &= \mathcal{U}_{16}^1 \otimes \mathcal{V}_{13}^1 \\
 &= \mathcal{X}_{16} \otimes \mathcal{K}_{16}^1 \otimes \mathcal{U}_4^2 \otimes \mathcal{K}_4^2 \\
 \mathcal{T}_2 &= \mathcal{U}_4^2 \otimes \mathcal{V}_1^2 \\
 &= \mathcal{U}_4^2 \otimes \mathcal{U}_1^3 \otimes \mathcal{K}_1^3 \\
 \mathcal{T}_3 &= \mathcal{U}_1^3 \otimes \mathcal{V}_1^3 \otimes \mathcal{V}_3^3 \\
 &= \mathcal{U}_1^3 \otimes \mathcal{U}_1^4 \otimes \mathcal{K}_1^4 \otimes \mathcal{U}_9^4 \otimes \mathcal{K}_9^4 \\
 \mathcal{T}_1 \otimes \mathcal{T}_2 \otimes \mathcal{T}_3 &= \mathcal{X}_{16} \otimes \mathcal{K}_{16}^1 \otimes \mathcal{U}_4^2 \otimes \mathcal{K}_4^2 \otimes \mathcal{U}_4^2 \otimes \mathcal{U}_1^3 \otimes \mathcal{K}_1^3 \otimes \mathcal{U}_1^3 \otimes \mathcal{U}_1^4 \otimes \mathcal{K}_1^4 \otimes \mathcal{U}_9^4 \otimes \mathcal{K}_9^4 \\
 &= \mathcal{X}_{16} \otimes \mathcal{U}_1^4 \otimes \mathcal{U}_9^4 \otimes \mathcal{K}_9^4 \otimes \mathcal{K}_{16}^1 \otimes \mathcal{K}_1^4 \otimes \mathcal{K}_4^2 \otimes \mathcal{K}_1^3
 \end{aligned}$$

(die letzte Zeile ergibt sich durch das wegheben einzelner Zufallsvariablen gegeneinander). Da man davon ausgeht, dass der Schlüssel eine feste Grösse ist, insbesondere also auch die Schlüsselbits verknüpft entweder 0 oder 1 ergeben (siehe Skript in 3.5), ist der Bias von $\mathcal{X}_{16} \otimes \mathcal{U}_1^4 \otimes \mathcal{U}_9^4$ also $\pm \frac{1}{16}$, wobei das Vorzeichen vom Schlüssel abhängig ist.

Alternativ hätte man auch über S_2^2 gehen können, was ein Bias von $\frac{1}{64}$ ergeben hätte, mit gleicher Anzahl von relevanten S-Boxen.

- (b) Die lineare Attacke ist nach der Vorarbeit in 10(a) nun recht einfach : Die Zufallsvariable $\mathcal{X}_{16} \otimes \mathcal{U}_1^4 \otimes \mathcal{U}_9^4$ hat ein zur Attacke verwendbares deutliches Bias von $\pm \frac{1}{16}$. Herauszubekommen sind nun die acht Schlüsselbits $\mathcal{K}_{(1)}^5$ und $\mathcal{K}_{(3)}^5$, da diese mit dem Output der beiden relevanten S-Boxen S_1^4 und S_3^4 mittels \otimes verknüpft werden; Der verwendete Algorithmus ist im Skript bereits genauer unter (3.7) und in Abbildung 3.5 angegeben und funktioniert hier exakt analog mit dem Unterschied, dass der Bias hier sogar $\pm \frac{1}{16}$ anstatt $\pm \frac{1}{32}$ beträgt.
- (c) Der in 10(b) angedeutete Algorithmus wurde von uns in spnbreaker implementiert. Es werden ungefähr $c \cdot \epsilon^{-2}$ Paare benötigt in diesem Fall ca. 4500-5500 Text. (Was in etwa der Verbesserung entspricht die durch die wesentlich bessere Verzerrung entsteht).

Aufgabe 19

Generell ist eine Funktion f linear, wenn $f(a + b) = f(a) + f(b)$ gilt. Somit ist die Nicht-Linearität von DES-S-Box S_4 (hier als Funktion aufgefasst) einfach durch ein Gegenbeispiel zu widerlegen : $S_4(000010 \otimes 000001) = S_4(000011) = 1000 \neq 0000 = 1101 \otimes 1101 = S_4(000010) \otimes S_4(000001)$

Anhang

Unser Source-Repository zu den Kryptographie-Übungszetteln ist auch unter [HTTP://SVN.WIREBRAIN.DE:8080/KRYPTO.CGI](http://svn.wirebrain.de:8080/krypto.cgi) zugänglich.

```

#!/usr/local/bin/perl -w
use strict;
use Number::Fraction;

#SPN S-Box vom Uebungszettel
my @pi_s = (0x8, 0x4, 0x2, 0x1, 0xc, 0x6, 0x3, 0xd,
            0xa, 0x5, 0xe, 0x7, 0xf, 0xb, 0x9, 0x0);

my @reverse_pi_s = (0xf, 0x3, 0x2, 0x6, 0x1, 0x9, 0x5, 0xb,
                    0x0, 0xe, 0x8, 0xd, 0x4, 0x7, 0xa, 0xc);

#Original SPN S-Box aus Skript
#my @pi_s = (0xe, 0x4, 0xd, 0x1, 0x2, 0xf, 0xb, 0x8,
#            0x3, 0xa, 0x6, 0xc, 0x5, 0x9, 0x0, 0x7);

my @pi_p = (0, 4, 8, 12, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15);

my @k = (0,0,1,1, 1,0,1,0, 1,0,0,1, 0,1,0,0,
         1,1,0,1, 0,1,1,0, 0,0,1,1, 1,1,1,1);

my @nl = map {
    my @t;
    for my $a (0..15) { for my $b (0..15) { $t[$a][$b] = 16 }}

    for (0..15) {
        my @l = (split (//, sprintf '%04b', $_),
                 substitute (split //, sprintf '%04b', $_));
        for my $a (0..15) {
            for my $b (0..15) {
                my @j = (split (//, sprintf '%04b', $a),
                         split (//, sprintf '%04b', $b));
                my $r = 0;
                $j[$_] and $r ^= $l[$_] for 0..7;
                $t[$a][$b] -= $r
            }
        }
    }
    @t
}1;

sub substitute {
    split //, sprintf '%04b', $pi_s[oct 'b'.join '', @_]
}

sub reversesubstitute {
    split //, sprintf '%04b', $reverse_pi_s[oct 'b'.join '', @_]
}

sub SPN {
    my @w = @_;

```

```

for my $i (0..2) {
    $w[$_ - $i*4] ^= $k[$_] for $i*4..$i*4+15;
    my @v; push @v, substitute (splice @w, 0, 4) for 0..3;
    $w[$_] = $v[$pi_p[$_]] for 0..15
}
$w[$_ - 12] ^= $k[$_] for 12..27;
my @v; push @v, substitute (splice @w, 0, 4) for 0..3;
$v[$_ - 16] ^= $k[$_] for 16..31;
@v
}

sub SPNBreaker {
    my %pairs = %{{shift ()}};
    my %count = ();

    for my $i (0..15) {
        for my $j (0..15) {
            $count {($i,$j)} = 0
        }
    }

    for my $pt (keys %pairs) {
        for my $ref (keys %count) {
            my @L1 = split //, sprintf '%04b', $ref->[0];
            my @L2 = split //, sprintf '%04b', $ref->[1];
            my @v41; push @v41, $L1[$_] ^ $pairs{$pt}->[$_] for 0..3;
            my @v43; push @v43, $L2[$_-8] ^ $pairs{$pt}->[$_] for 8..11;

            my @u41 = reversesubstitute @v41;
            my @u43 = reversesubstitute @v43;

            my $z = $pt->[16] ^ $u41[0] ^ $u43[0];
            $count{@$ref} += 1 unless $z;
        }
    }

    my $max = 0; my $maxkey = 0;

    for my $ref (keys %count) {
        if ($count {@$ref} - 1/2 * scalar keys %count > $max) {
            $max = $count {@$ref} - 1/2 * scalar keys %count;
            $maxkey = $ref
        }
    }

    @$maxkey;
}

sub f { Number::Fraction->new ($_[0], $_[1]) }

```

```

sub tf { 'f' . join '', map { '{' . $_ . '}' } split '/', shift }

sub prob17a {
  my (%p, %e);
  $p{$_}{Pasch} = $p{$_}{NichtPasch} = $e{$_} = 0 for 2..12;
  $e{Pasch} = $e{NichtPasch} = 0;
  foreach my $x1 (1..6) {
    foreach my $x2 (1..6) {
      $e{$x1+$x2}++;
      $p{$x1+$x2}{Pasch}++, $e{Pasch}++ if $x1 == $x2;
      $p{$x1+$x2}{NichtPasch}++, $e{NichtPasch}++ unless $x1 == $x2
    }
  }
  print '$';
  foreach my $x (2..12) {
    for my $y ('Pasch', 'NichtPasch') {
      $_ = "p[$y,$x] = ".tf (f ($p{$x}{$y}, 36)).', '.
      "p[$y|$x] = f{p[$y,$x]}{p[$x]} = f{" .
      tf (f ($p{$x}{$y}, 36)).'}{'.tf (f ($e{$x}, 36)).'} = '.
      tf (f ($p{$x}{$y}, 36) / f ($e{$x}, 36)) . ', '.
      "p[$x|$y] = f{p[$x,$y]}{p[$y]} = f{" .
      tf (f ($p{$x}{$y}, 36)).'}{'.tf (f ($e{$y}, 36)).'} = '.
      tf (f ($p{$x}{$y}, 36) / f ($e{$y}, 36));
      s/p/\mathcal{P}/g; s/f/\frac/g;
      s/\[/\left[/g; s/\]/\right[/g;
      s/\frac\{0\}\{1\}/0/g; s/\frac\{1\}\{1\}/1/g;
      s/NichtPasch/\mathrm{NP}/g; s/Pasch/\mathrm{P}/g;
      print $_, $x%12 ? '\\\\' : '', "\n";
    }
  }
  print '$'
}

my %des = ( 1 => [[14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7],
  [0,15,7,4,14,2,13,1,10,6,12,11,9,5,3,8],
  [4,1,14,8,13,6,2,11,15,12,9,7,3,10,5,0],
  [15,12,8,2,4,9,1,7,5,11,3,14,10,0,6,13]],
  2 => [[15,1,8,14,6,11,3,4,9,7,2,13,12,0,5,10],
  [3,13,4,7,15,2,8,14,12,0,1,10,6,9,11,5],
  [0,14,7,11,10,4,13,1,5,8,12,6,9,3,2,15],
  [13,8,10,1,3,15,4,2,11,6,7,12,0,5,14,9]],
  3 => [[10,0,9,14,6,3,15,5,1,13,12,7,11,4,2,8],
  [13,7,0,9,3,4,6,10,2,8,5,14,12,11,15,1],
  [13,6,4,9,8,15,3,0,11,1,2,12,5,10,14,7],
  [1,10,13,0,6,9,8,7,4,15,14,3,11,5,2,12]],
  4 => [[7,13,14,3,0,6,9,10,1,2,8,5,11,12,4,15],
  [13,8,11,5,6,15,0,3,4,7,2,12,1,10,14,9],
  [10,6,9,0,12,11,7,13,15,1,3,14,5,2,8,4],
  [3,15,0,6,10,1,13,8,9,4,5,11,12,7,2,14]],
  5 => [[2,12,4,1,7,10,11,6,8,5,3,15,13,0,14,9],

```

```

        [14,11,2,12,4,7,13,1,5,0,15,10,3,9,8,6],
        [4,2,1,11,10,13,7,8,15,9,12,5,6,3,0,14],
        [11,8,12,7,1,14,2,13,6,15,0,9,10,4,5,3]],
6 => [[12,1,10,15,9,2,6,8,0,13,3,4,14,7,5,11],
      [10,15,4,2,7,12,9,5,6,1,13,14,0,11,3,8],
      [9,41,15,5,2,8,12,3,7,0,4,10,1,13,11,6],
      [4,3,2,12,9,5,15,10,11,14,1,7,6,0,8,13]],
7 => [[4,11,2,14,15,0,8,13,3,12,9,7,5,10,6,1],
      [13,0,11,7,4,9,1,10,14,3,5,12,2,15,8,6],
      [1,4,11,13,12,3,7,14,10,15,6,8,0,5,9,2],
      [6,11,13,8,1,4,10,7,9,5,0,15,14,2,3,12]],
8 => [[13,2,8,4,6,15,11,1,10,9,3,14,5,0,12,7],
      [1,15,13,8,10,3,7,4,12,5,6,11,0,14,9,2],
      [7,11,4,1,9,12,14,2,0,6,10,13,15,3,5,8],
      [2,1,14,7,4,10,8,13,15,12,9,0,3,5,6,11]]);

sub prob17c {
  sub dsubstitute {
    split //, sprintf '%04b', $des{$_[0]}->
      [oct'b'.'$_[1].$_[6]]->
      [oct'b'.join'',splice @_,2,4];
  }

  for my $box (1..8) {
    my $t = 64;
    for (0..63) {
      @_ = (split (//, sprintf '%06b', $_),
            dsubstitute ($box, split //, sprintf '%06b',$_));
      $t -= $_[1] ^ $_[6] ^ $_[7] ^ $_[8] ^ $_[9];
    }
    print "DES S-Box $box Bias fuer X22Y11Y22Y33Y44: ",
          (f($t,64) - f(1,2)), "\n";
  }
}

prob17a if $ARGV[0] eq 'prob17a';
prob17c if $ARGV[0] eq 'prob17c';
if ($ARGV[0] eq 'spn') {
  print SPN (0,0,1,0, 0,1,1,0, 1,0,1,1, 0,1,1,1), "\n";
}

if ($ARGV[0] eq 'nl') {
  print "  0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F\n";
  for my $i (0..15) {
    print sprintf ("%1x ", $i);
    for my $j (0..15) {
      print sprintf ('%2d', $nl[$i][$j]), " "
    }
    print "\n"
  }
}

```

```
}  
  
if ($ARGV[0] eq 'prob18a') {  
    print $n1[1][4], " ", $n1[1][8], " ", $n1[4][10];  
}
```