Ausnutzen von S-Box-Eigenschaften

$$S^{-1}(c_0 \oplus k_2) \oplus S^{-1}(c_1 \oplus k_2) = S(m_0 \oplus k_0) \oplus S(m_1 \oplus k_0) \quad (*)$$

bei Cipher ONE: fester Wert

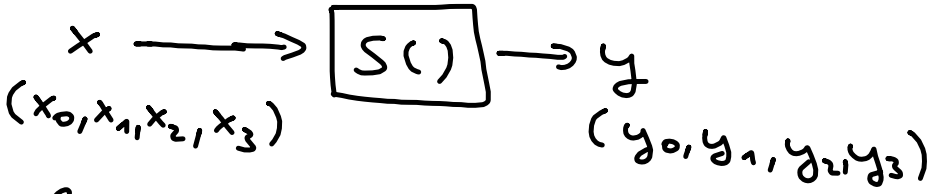
Cipher TWO: Ausnutzen der Differenzen

Strategie:

- Differenzen mit hohen Wahrscheinlichkeitswerten in DDT finden (Diff. Distribution Table)
  z.B. 10/16 bei Input-Diff. 0xf und Output-Diff 0xd
- erzeuge Eingabe-/Ausgabepaare (PT-CT-pairs) m, m' mit $m' = m \oplus 0xf$ und zugehörigen c, c'
- zähle für jeden Wert k_2, wie oft die linke Seite von $(*)$ der Output-Differenz 0xd der S-Box entspricht.

Lineare Kryptoanalyse

Ziel: lineare Darstellung der S-Box
in einer vorgegebenen Häufigkeit von Fällen



linearer Zusammenhang:

$$a_0 \cdot x_0 \oplus a_1 \cdot x_1 \oplus a_2 \cdot x_2 \oplus a_3 \cdot x_3$$

$$= b_0 \cdot y_0 \oplus b_1 \cdot y_1 \oplus b_2 \cdot y_2 \oplus b_3 \cdot y_3$$

für alle $a_i, b_i \in \{0,1\}$ und alle Eingaben x ($\rightarrow y = S(x)$)

→ LDT linear distribution table

Interessant sind in der LDT

a) große Werte

b) kleine Werte

zu a) $3 \to 3$ in 52/256 Fällen

$(a_3, a_2, a_1, a_0) \to (b_3, b_2, b_1, b_0)$

0 0 1 1 0 0 1 1

$$x_1 \oplus x_0 = y_1 \oplus y_0$$

die x_i, y_i enthalten algebraischen Ausdrücke in den Keybits (k_0, k_1, k_2)

$k_{03}, k_{02}, k_{01}, k_{00}$

zu b)

wenn kleiner LDT-Wert, z.B.

lineare Gleichung in 4% der Fälle erfüllt

z.B. Input 0xc, Output 0xc

1 1 0 0 1 1 0 0

$x_3 \oplus x_2 = y_3 \oplus y_2$ in 4% der Fälle

$\Downarrow$

$x_3 \oplus x_2 = y_3 \oplus y_2 \oplus 1$ ← in 96% der Fälle

$\Rightarrow$ Gleichungen in $k_{00}, \ldots, k_{23}$

jede Gleichung ergibt eines der Keybits

⇝ es sind so viele Gleichungen nötig, dass der Rest der Keybits ausgezählt werden kann

z.B.