Differentielle Kryptoanalyse

Cipher ONE

$$c = S(m + k_0) + k_1$$

DDT

Input - Output - Differenzen von S

$m_2 = m_1 + d_1$

$S(m_1) + S(m_2) = d_2$

Cipher TWO

2 x S-Box

3 x key addition

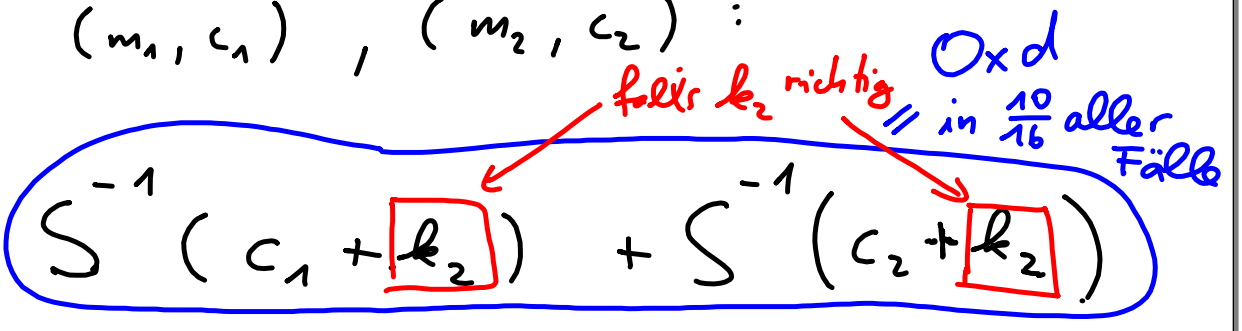
$$c = S(S(m + k_0) + k_1) + k_2$$

$$c + k_2 = S(S(m + k_0) + k_1)$$

$$S^{-1}(c + k_2) = S(m + k_0) + k_1$$

Für ein plaintext-ciphertext-Paar

(m_1, c_1) , (m_2, c_2) :



$= S(m_1 + k_0) + k_1 + S(m_2 + k_0) + k_1$

$m_1 + m_2 = d_1$ vorgeben, z.B. 0x f

Ziel:

für alle Teilschlüssel k_2 berechne die Häufigkeit, mit der vorige Gleichung erfüllt ist.

Tue dies für alle (m_1, m_2)-Paare mit $m_1 + m_2 = d$.

Falls Häufigkeit = Wahrscheinlichkeit $\Rightarrow$ k_2 Kandidat

$\Rightarrow$ cipher TWO um eine Runde reduziert

$\rightsquigarrow$ attackiere cipher ONE

---

cipher THREE

3x S-Box S^{-1} $S(S(S(\ldots)))$

2x ! DT

Differenz: $0xf \overset{\frac{10}{16}}{\rightsquigarrow} 0xd \overset{\frac{6}{16}}{\rightsquigarrow} 0xc$ ~~differential~~ path"

Wahrscheinlichkeit, nach 2 S-Box-Aufrufen

$$\square f \rightsquigarrow \square c$$ zu erhalten

ist

$$\frac{10}{16} \cdot \frac{6}{16} = \frac{60}{256} = \frac{15}{64} \approx 25\,\%$$

⇒ suche differentielle Pfade mit hoher Wahrscheinlichkeit