Blockchiffren

cipher ONE siehe Folie

$$c = S(m \oplus k_0) \oplus k_1$$

bei zwei Klartexten / Chiffretexten

$$c_1 = S(m_1 \oplus k_0) \oplus k_1$$
$$c_2 = S(m_2 \oplus k_0) \oplus k_1$$

$\oplus$

$$\Rightarrow c_1 \oplus c_2 = S(m_1 + k_0) \oplus k_1$$

$$\oplus S(m_2 \oplus k_0) \oplus k_1$$

$$c_1 \oplus c_2 = S(m_1 \oplus \underbrace{k_0}) \oplus S(m_2 \oplus \underbrace{k_0})$$

4 Bit $\to 2^4$ Versuche

vorher: $(k_0, k_1) \rightsquigarrow 2^8$ Versuche

Attackierungsmodelle:

Angreifer kennt Key k nicht

1) known-plaintext-attack

Angreifer kennt (einige) Klartexte mit zugehörigen Chiffretexten

2) chosen-plaintext-attack

Angreifer kann sogar Klartexte wählen

3) chosen-ciphertext-attack

Differenzielle Kryptoanalyse

Idee:

Angreifer gibt Klartexte mit vorgegebenen Differenz d vor

$$d = m_1 \oplus m_2$$

$\rightsquigarrow$ chosen plaintext attack

$$m_2 = m_1 \oplus d$$

Anwendung auf Cipher ONE:

$$\underline{\quad \oplus k_1}) \oplus k_0 \oplus S^{-1}(\underline{c_2 \oplus k_1}) \oplus k_0$$

$$= S^{-1}(c_1 \oplus k_1) \oplus S^{-1}(c_2 \oplus k_1) = \underbrace{m_1 \oplus m_2 = d}_{\text{Eingabedifferenz für } S(\ )}$$

$c_1 \oplus c_2$

Ausgabedifferenz für $S(\ )$

$S^{-1}(c_1$

Difference Distribution Table (DDT)

listet Eingabedifferenzen und Ausgabedifferenzen

$$\mathrm{DDT} \quad \begin{array}{cc} d \rightarrow & \begin{pmatrix} & \vdots & \\ \cdots & D_{dd'} & \cdots \\ & \vdots & \end{pmatrix} \\ & \uparrow \\ & d' \end{array}$$

Erzeugung der DDT-Werte

for all m_1 do
  for all d do
    $m_2 = m_1 \oplus d$
    $d' = S(m_1) \oplus S(m_2)$
    $D_{dd'} = D_{dd'} + 1$
  od
od

Interessant sind "große" Werte

als Wahrscheinlichkeit

$$\underbrace{d \leadsto d'}_{\text{Übergang von Eingabedifferenz } d \text{ zu Ausgabedifferenz } d'}$$

Wahrscheinlichkeit $\frac{D}{2^n}$, n Blocklänge für $S(\,)$

Übung:

- cipher ONE implementieren
- testen
- DDT erzeugen