

Blockchiffren

Cipher ONE siehe Folie

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

bei zwei Klartexten / Chiffretexten

$$C_1 = S(m_1 \oplus k_0) \oplus k_1$$

$$C_2 = S(m_2 \oplus k_0) \oplus k_1$$



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

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

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

vorher: $(k_0, k_1) \rightsquigarrow 2^8$ Versuche
 4 Bit $\rightarrow 2^4$ Versuche

Attachierungsmodelle:

Angreifer kennt Key & nicht

1) known-plaintext-attack

Angreifer kennt (einige) Klartexte
mit zugehörigen Chiffertexten

2) chosen-plaintext-attack

Angreifer kann sogar Klartexte wählen

3) chosen-ciphertext-attack

Differenzielle Kryptanalyse

Idee:

Angreifer gibt Klartexte mit vorgegebener

Differenz d vor

$$d = m_1 \oplus m_2$$

$$\hookrightarrow m_2 = m_1 \oplus d$$

→ chosen plaintext attack

Anwendung auf Cipher ONE:

$$\begin{aligned}
 & \oplus k_1) \oplus k_0 \oplus S^{-1}(c_2 \oplus k_1) \oplus k_0 \\
 = & S^{-1}(c_1 \oplus k_1) \oplus S^{-1}(c_2 \oplus k_1) = \underbrace{m_1 \oplus m_2}_{\substack{\text{Eingabedifferenz} \\ \text{für } S()}} = d
 \end{aligned}$$

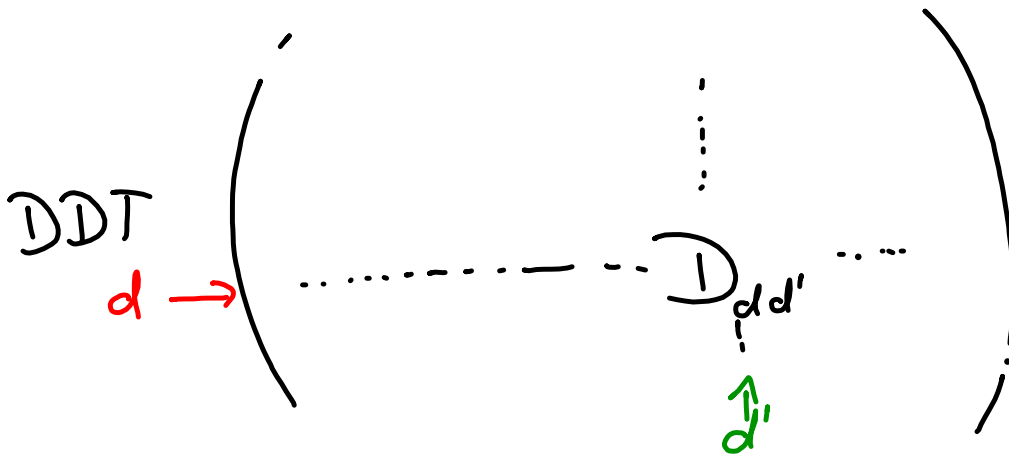
$$c_1 \oplus c_2$$

Ausgabedifferenz für $S()$

$$S^{-1}(c_1$$

Difference Distribution Table (DDT)

listet Eingabedifferenzen und Ausgabedifferenzen



Erzeugung der DDT-Werte

for all m_1 do

for all d do

$$m_2 = m_1 \oplus d$$

$$d' = S(m_1) \oplus S(m_2)$$

$$D_{dd'} = D_{d'd} + 1$$

od

od

Interessant sind "große" Werte
als Wahrscheinlichkeit

$$d \rightsquigarrow d'$$

Übergang von Eingabedifferenz d
zu Ausgabedifferenz d'
Wahrscheinlichkeit $\frac{D}{2^n}$, n Bits Dinge
für $S(i)$

Übung:

- cipher ONE implementieren
- teilen
- DDT erzeugen