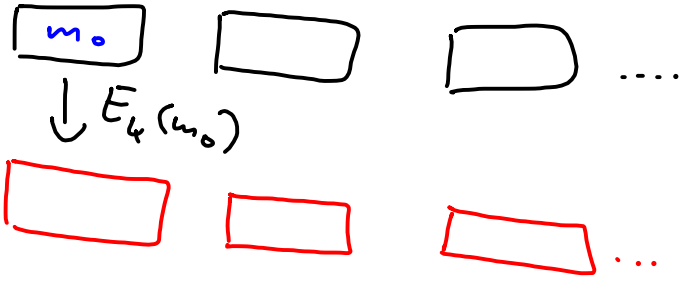
Blockchiffren

(und Kryptoanalyse)



Beispiel:

Cipher ONE

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

$= E_k(m)$ mit $k = (k_0, k_1)$

Beispiel:
$E_{0x37}(0xd1) = 0x7$

Entschlüsselung:

Verschlüsselung schrittweise rückgängig machen

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

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

$c \oplus k_1 = S(m \oplus k_0) \quad \| S^{-1}(\,)$

$S^{-1}(c \oplus k_1) = m \oplus k_0$

$m = S^{-1}(c \oplus k_1) \oplus k_0$

Attacke:

1. Brute force: alle Keys ausprobieren (hier 2^8)
2. Differenzen betrachten

Differentielle Kryptoanalyse

funktioniert für

plaintext - ciphertext - pairs

(m_0, c_0) , (m_1, c_1)

verschlüsselt mit gleichem Schlüssel

$$m_0 = S^{-1}(c_0 \oplus k_1) \oplus k_0$$
$$m_1 = S^{-1}(c_1 \oplus k_1) \oplus k_0$$

$\oplus$ "Differenz"

$$m_0 \oplus m_1 = S^{-1}(c_0 \oplus k_1) \oplus S^{-1}(c_1 \oplus k_1)$$

→ Brute-Force reduziert auf 2^4 Schritte

→ k_1

→ u

$m \oplus k_0 = u \Rightarrow k_0 = u \oplus m$

Erweiterung auf mehrere Runden

≙ mehrmaliges Anwenden der S-Box $S()$

$$c = S(S(m \oplus k_0) \oplus k_1) \oplus k_2$$

Attacke:

wieder PT-CT-pairs $(m_0, c_0), (m_1, c_1)$

$$m_0 = S^{-1}(S^{-1}(c_0 \oplus k_2) \oplus k_1) \oplus k_0$$
$$m_1 = S^{-1}(S^{-1}(c_1 \oplus k_2) \oplus k_1) \oplus k_0$$

$\oplus$ (1. Versuch)

$$m_0 \oplus m_1 = S^{-1}(S^{-1}(c_0 \oplus k_2) \oplus k_1) \oplus S^{-1}(S^{-1}(c_1 \oplus k_2) \oplus k_1)$$

$| S()$

2. Versuch:

$$m_0 \oplus k_0 = S^{-1}(S^{-1}(c_0 \oplus k_2) \oplus k_1) \quad \| S()$$

$$S(m_0 \oplus k_0) = S^{-1}(c_0 \oplus k_2) \oplus k_1$$
$$S(m_1 \oplus k_0) = S^{-1}(c_1 \oplus k_2) \oplus k_1$$

↑ Differenzen bilden (Input)

$$(m_0 \oplus k_0) \oplus (m_1 \oplus k_0) = m_0 \oplus m_1$$

danach protokolliert man für die S-Box, wie oft für eine bestimmte Eingabedifferenz x eine bestimmte Ausgabedifferenz y entsteht, d.h.

```
for all m1, m2
{   x = m1 ⊕ m2
    y = S(m1) ⊕ S(m2)
    diff [x, y] ++
}
```

diff [ ] difference distribution table