htw saar

Studiengang Kommunikationsinformatik (Master)
Studiengang Praktische Informatik (Master)
Prof. Dr.–Ing. Damian Weber

Example Ciphers

Differential Cryptanalysis

1 Cipher ONE

The S–box of cipher ONE is

```
            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
sbox      : 06 04 0c 05 00 07 02 0e 01 0f 03 0d 08 0a 09 0b

            00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
sbox^{-1}: 04 08 06 0a 01 03 00 05 0c 0e 0d 0f 02 0b 07 09
```

Algorithms E and D of cipher ONE work as follows:

- $E_k(m)$
  (1) $u = m \oplus k_0$
  (2) $v = S(u)$
  (3) $c = v \oplus k_1$
  (4) return c
- $D_k(c)$
  (1) $v = c \oplus k_1$
  (2) $u = S^{-1}(v)$
  (3) $m = u \oplus k_0$
  (4) return m

For example encrypting with key $k = (k_0 k_1) = 0x97$ gives

$$\underbrace{0xd}_{m} \xrightarrow{k} \underbrace{0x7}_{c}.$$

2 Cipher TWO

Algorithms E and D of cipher TWO work as follows:

- $E_k(m)$
  (1) $u = m \oplus k_0$
  (2) $v = S(u)$
  (3) $w = v \oplus k_1$
  (4) $x = S(w)$
  (5) $c = x \oplus k_2$
  (6) return c
- $D_k(c)$
  (1) $x = c \oplus k_2$
  (2) $w = S^{-1}(x)$
  (3) $v = w \oplus k_1$
  (4) $u = S^{-1}(v)$
  (5) $m = u \oplus k_0$
  (6) return m

For example encrypting with key $k = 0x959$ gives

$$\underbrace{0xd}_{m} \xrightarrow{k} \underbrace{0xe}_{c}.$$