Cryptanalysis

Prof. Dr.-Ing. Damian Weber

Hochschule für Technik und Wirtschaft des Saarlandes

Blockchiffren: Aufbau

Iteration von

Konfusion (S-Box, bijektive Abb.)

Diffusion (Permutation von Bitpositionen)

= Runden … (Attacken auf reduzierte Rundenzahl)

Cipher ONE
with 1 non-linear component

4-Bit-Verschlüsselung mit 8-Bit-Key (k_0,k_1)

$E_k(m)$

(1) $u = m \oplus k_0$

(2) $v = S(u)$

(3) $c = v \oplus k_1$

(4) return c

Entschlüsselungs-

Funktion D(m) ?

		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

Cipher ONE
with 1 non-linear component

$E_k(m)$

(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

		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

Cipher TWO
with 2 non-linear components

4-Bit-Verschlüsselung mit 12-Bit-Key (k_0,k_1,k_2)

$E_k(m)$

(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

Entschlüsselungs-

Funktion D(m) ?

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

Cipher TWO
with 2 non-linear components

$E_k(m)$

(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

		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

Difference Distribution Table

	output	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
input	00 :	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
input	01 :	0	0	6	0	0	0	0	2	0	2	0	0	2	0	4	0
input	02 :	0	6	6	0	0	0	0	0	0	2	2	0	0	0	0	0
input	03 :	0	0	0	6	0	2	0	0	2	0	0	0	4	0	2	0
input	04 :	0	0	0	2	0	2	4	0	0	2	2	2	0	0	2	0
input	05 :	0	2	2	0	4	0	0	4	2	0	0	2	0	0	0	0
input	06 :	0	0	2	0	4	0	0	2	2	0	2	2	2	0	0	0
input	07 :	0	0	0	0	0	4	4	0	2	2	2	2	0	0	0	0
input	08 :	0	0	0	0	0	2	0	2	4	0	0	4	0	2	0	2
input	09 :	0	2	0	0	0	2	2	2	0	4	2	0	0	0	0	2
input	0a :	0	0	0	0	2	2	0	0	0	4	4	0	2	2	0	0
input	0b :	0	0	0	2	2	0	2	2	2	0	0	4	0	0	2	0
input	0c :	0	4	0	2	0	2	0	0	2	0	0	0	0	0	6	0
input	0d :	0	0	0	0	0	0	2	2	0	0	0	0	6	2	0	4
input	0e :	0	2	0	4	2	0	0	0	0	0	2	0	0	0	0	6
input	0f :	0	0	0	0	2	0	2	0	0	0	0	0	0	10	0	2

Cipher THREE
with 3 non-linear components

4-Bit-Verschlüsselung mit 16-Bit-Key (k_0,k_1,k_2,k_3)

$E_k(m)$

(1) $u = m \oplus k_0$
(2) $v = S(u)$
(3) $w = v \oplus k_1$
(4) $x = S(w)$
(5) $y = x \oplus k_2$
(6) $z = S(y)$
(7) $c = z \oplus k_3$
(8) return c

D( ) ?

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

Cipher THREE
with 3 non-linear components

4-Bit-Verschlüsselung mit 16-Bit-Key (k_0,k_1,k_2,k_3)

$E_k(m)$

$$
\begin{aligned}
&(1)\quad u = m \oplus k_0\\
&(2)\quad v = S(u)\\
&(3)\quad w = v \oplus k_1\\
&(4)\quad x = S(w)\\
&(5)\quad y = x \oplus k_2\\
&(6)\quad z = S(y)\\
&(7)\quad c = z \oplus k_3\\
&(8)\quad \text{return } c
\end{aligned}
$$

$D_k(c)$

$$
\begin{aligned}
&(1)\quad z = c \oplus k_3\\
&(2)\quad y = S^{-1}(z)\\
&(3)\quad x = c \oplus k_2\\
&(4)\quad w = S^{-1}(x)\\
&(5)\quad v = w \oplus k_1\\
&(6)\quad u = S^{-1}(v)\\
&(7)\quad m = u \oplus k_0\\
&(8)\quad \text{return } m
\end{aligned}
$$

		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