Krypto 1 GÜ 7

show IP, E, $\oplus K$, S, P are linear?

1.) IP

$$IP(a_1, a_2, \dots, a_{64}) = (a_{58}, a_{50}, \dots, a_7)$$
$$IP(b_1, b_2, \dots, b_{64}) = (b_{58}, b_{50}, \dots, b_7)$$

$$IP(a \oplus b) = (a_{58} \oplus b_{58}, a_{50} \oplus b_{50}, \dots, a_7 \oplus b_7)$$
$$= IP(a) \oplus IP(b) \Rightarrow IP \text{ linear!}$$

2.) E:

$$E(a_1, a_2, \dots, a_{32}) = (a_{32}, a_1, a_2, \dots, a_1)$$
$$E(\cancel{b_{32}}\, b_1, b_2, \dots, b_{32}) = (b_{32}, b_1, b_2, \dots, b_1)$$

$$E(a \oplus b) = (a_{32} \oplus b_{32}, \dots, b_1 \oplus a_1)$$
$$= E(a) \oplus E(b)$$
$$\Rightarrow \text{linear!}$$

3.) $\oplus K$: $(a \oplus k) \oplus (b \oplus k) = a \oplus k \oplus b \oplus k = a \oplus b$
$$\neq (a \oplus b) \oplus k$$

$\Rightarrow$ linear!

4.) S: $S_1(\underbrace{0}_{\text{column}}\overbrace{0\,0\,0\,0}^{\text{row}}0) \oplus S_1(000001)$

$$= 1110 \oplus 0100 = 1010 \longleftarrow \neq$$

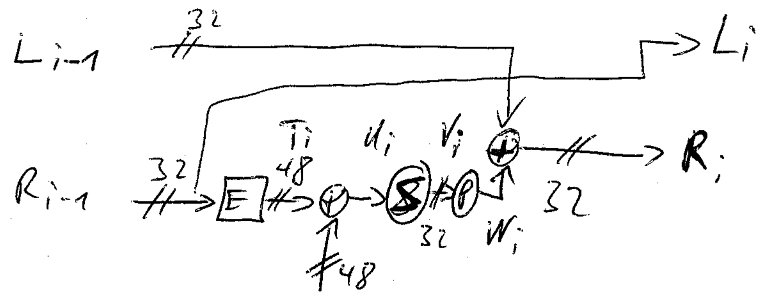
$$S_1(000000 \oplus 000001) = S_1(000001) = \underline{0100}$$

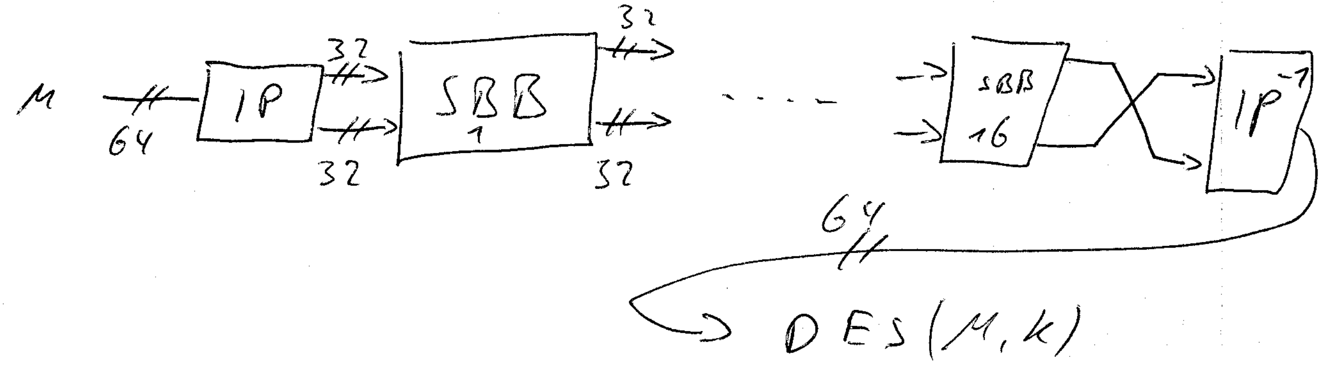
$\Rightarrow$ non-linear!

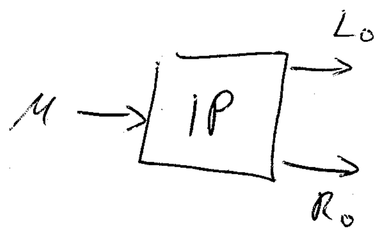
S.1 ⇒ linear since IP is linear

a) Show that $DES(M,k) = \overline{DES(\bar{M},\bar{k})}$

SBB







- $IP(\bar{M}) = (\bar{L}_0, \bar{R}_0)$ // permutation doesn't affect the complementation
- $E(\overline{R_{i-1}}) = \overline{E(R_{i-1})}$

// the double bits are complemented

- $\bar{T}_i \oplus \bar{k}_i = T_i \oplus k_i$

⇒ $S(U_i)$ doesn't change

⇒ $P(V_i)$ – " –

$W_i \oplus \overline{L_{i-1}} = \bar{R}_i$

$L_i \Rightarrow \overline{R_{i-1}} = \bar{L}_i$ ⇒ $SBB(\bar{R}_i, \bar{L}_i) = \overline{SBB(R_i, L_i)}$

This is done for 16 iterations

$\Rightarrow IP^{-1}(R_{16}, L_{16}) = DES(\bar{M}, \bar{k})$

$= \overline{DES(M,k)}$

Crypt 1 Gü 7

$\Rightarrow \overline{DES(\bar{m}, \bar{k})} = DES(m, k)$

b.) In a brute force attack, the amount of calculations is halvened.

Ex 22 Linear Feedback Shift Register (LFSR) based stream cipher

Message $m = m_1, m_1, m_l \in \mathbb{F}_2^l$

key $k = k_1, \ldots, k_n \in \mathbb{F}_2^l$ $n < l$

Keystream $z = z_1, \ldots, z_l$

$z_i = k_i$ $1 \leq i \leq n$

$z_i = \sum_{j=1}^{n} s_j z_j \pmod 2$ $n \leq i \leq l$

$c_i = m_i \oplus z_i$ $1 \leq i \leq l$

a.) Decryption

$m_i = c_i \oplus z_i$ $\Rightarrow$ Encryption = Decryption

b.)

$k = 0 \ldots 0 \Rightarrow z_i = 0$ $1 < i < n$

$z_i = 0$ $n < i < l$

$\Rightarrow c_i = m_i$

$\Rightarrow$ plaintext is not encrypted

c.) $n = 4$, $s_1 = s_4 = 1$, $s_2 = s_3 = 0$, $l = 20$

$k = 0110$

z_1	z_2	z_3	z_4	z_5	z_6	7	8	9	10	11	12	13	14	15	16
0	1	1	0	0	1	0	0	0	1	1	1	1	0	1	0

$\oplus$

17	18	19	20
1	1	0	0