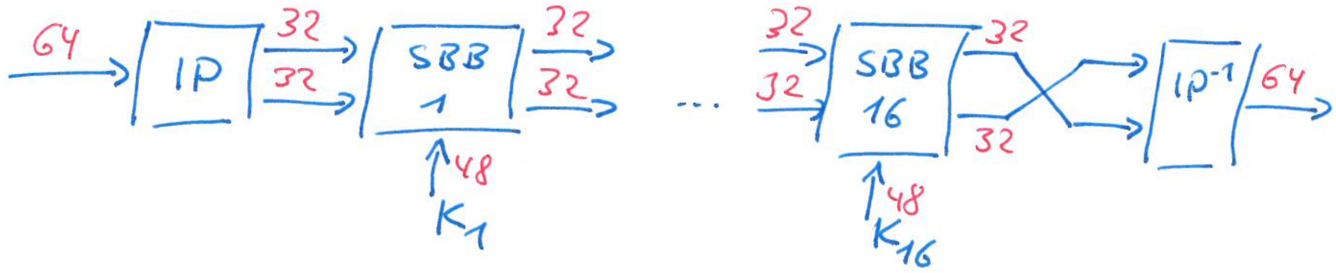
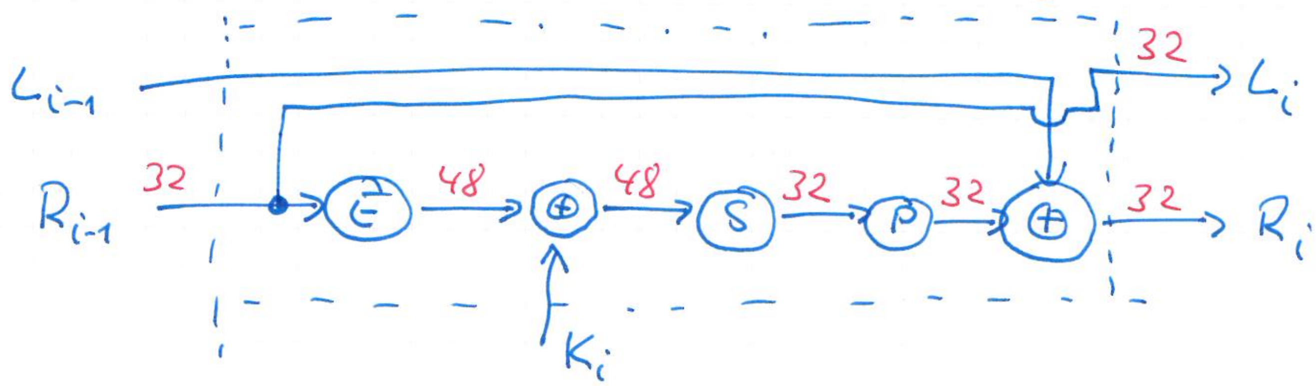
## 5.1.2 DES Encryption

Plaintext of 64 bits (otherwise group into blocks)




- IP ($IP^{-1}$) initial permutation (inverse) splitting into 2 blocks of 32 bits.
- SBB $i$, $i = 1, \dots, 16$, standard building block no. $i$




Formally: $L_i = R_{i-1}$ $\quad i = 1, \dots, 16$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

E: expansion map, permutation, 16 bits are doubled

⊕ : XOR, add. mod 2

P : permutation

RWTH AACHEN UNIVERSITY

$S$ : transformation $\{0,1\}^{48} \to \{0,1\}^{32}$

48 bits are partitioned into 8 blocks of 6 bits

$B = (B_1, \dots, B_8)$ , $B_i = (b_{i1}, b_{i2}, \dots, b_{i5}, b_{i6})$, $i = 1, \dots, 8$

$$S_i(B_i) = \text{bin}\left(a^{(i)}_{\text{dec}(b_{i1}, b_{i6}),\, \text{dec}(b_{i2}, b_{i3}, b_{i4}, b_{i5})}\right)$$

$a^{(i)}_{k\ell}$ : $(k,\ell)$th entry of $S_i$ (S-boxes)

$$S(B) = (S_1(B_1), \dots, S_8(B_8))$$

Ex.: $B_5 = (\hat{1}\dot{0}\dot{1}\dot{0}\dot{1}\hat{0})$

$10 \mathrel{\hat{=}} 2$ $\qquad a^{(5)}_{2,5} = 13$

$0101 \mathrel{\hat{=}} 5$

$\text{bin}(13) = (1101)$

## 5.1.3. DES Decryption

It holds $L_i = R_{i-1}$ , $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ , $i = 1, \dots, 16$

Hence $R_{i-1} = L_i$ , $L_{i-1} = R_i \oplus f(L_i, K_i)$ , $i = 1, \dots, 16$

$R_{16}$, $L_{16}$ are interchanged in the last step.

Hence, the same alg. can be used for decryption with the order of the keys interchanged.

Thinking the Future
Zukunft denken

## 5.1.4. Security of DES

- Design criteria of S-boxes unpublished.
- An IBM proposal was modified by NSA.
  Trapdoor by IBM avoided?
  Trapdoor built in by NSA? (non-confirmed)

DES is vulnerable to mainly 2 attacks.

[D. Coppersmith, IBM J. Res. Develop., vol. 38, no. 3, May 94, p. 243-250]

- Differential cryptanalysis
  [Book: Biham, Diff. cryptanalysis of the DES, Springer, 2011]
  [Biham & Shamir CRYPTO 92] [Stinson, 02, p. 89 ff.]
  S-boxes are optimized against diff. cryptanalysis.
  Method was known to IBM researchers 20 years ago?
  Factor 512 ~~fa~~ faster than brute force = exhaustive search.
- Exhaustive search ($2^{56}$ keys)
  1977: Diffie & Hellman proposed a machine that could break DES in one day. Estimated costs US$ 20 million. never built.
  1998: DES-cracker by EFF
  US$ 250'000, appr. 2 days
  2006: COPACOBANA (Bochum, Kiel)
  120 FPGAs, \$ 10'000, 6.4 days
  2008: COPACOBANA RIVYERA
  less ~~one~~ than one day
  2016: https://crack.sh
  online tool, promise 25 sec. on average using storage & side information.

## 5.1.5. Triple DES

Main criticism: key too short (56 bits)

Apply DES three times with different key. 2 variants:

Key: $(K_1, K_2, K_3)$ (168 bit):

$$C = DES_{K_3}\left(DES_{K_2}^{-1}\left(DES_{K_1}(M)\right)\right)$$

Key: $(K_1, K_2)$ (112 bits)

$$C = DES_{K_1}\left(DES_{K_2}^{-1}\left(DES_{K_1}(M)\right)\right)$$

$DES^{-1}$ to ensure compatibility with DES.

## 5.2. The Advanced Encryption Standard (AES)

Sept. 1997: NIST asked for the replacement of DES.

Requirements: Block length 128 bits, support of key lengths 128, 192, 256 bits

Deadline: June 98.

21 submitted proposals: After 3 AES-conferences Rijndael (authors Daemen & Rijmen, Leuven) was chosen in an open & fair way.

The 5 finalists were

MARS (IBM), RC6 (RSA), Rijndael (s. above)

Serpent (Biham et al.), Twofish (Schneier et. al.)

All are very strong.

Description of AES.

Computatations are mainly in the Field

$$\mathbb{F}_{2^8} = GF(2^8).$$

(Polynomials over $\mathbb{F}_2 = GF(2)$ reduced modulo $x^8 + x^4 + x^3 + x + 1$. (irreducible).

$$(1\ 1\ 0\ 1\ 0\ 1\ 0\ 1) \cdot (1\ 1\ 0\ 0\ 0\ 0\ 0\ 1) = (1\ 0\ 1\ 1\ 1\ 1\ 0\ 1)$$

$$(y^7 + y^6 + y^4 + y^2 + 1)(y^7 + y^6 + 1) =$$

$$y^{14} + \cancel{y^{13}} + y^{11} + y^9 + \cancel{y^7} + \cancel{y^{13}} + y^{12} + y^{10} + y^8 + \cancel{y^6}$$
$$+ \cancel{y^7} + \cancel{y^6} + y^4 + y^2 + 1$$

$$(y^{14} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^4 + y^2 + 1) : (y^8 + y^4 + y^3 + y + 1) = y^6 + y^4 + y^3$$

$$\underline{y^{14} \qquad + y^{10} + y^9 + y^7 + y^6}$$
$$y^{12} + y^{11} + y^8 + y^7 + y^6 + y^4 + y^2 + 1$$
$$\underline{y^{12} + y^8 + y^7 + y^5 + y^4}$$
$$y^{11} + y^6 + y^5 + y^2 + 1$$
$$\underline{y^{11} + y^7 + y^6 + y^4 + y^3}$$
$$y^7 + y^5 + y^4 + y^3 + y^2 + 1$$

$$(1\ 0\ 1\ 1\ 1\ 1\ 0\ 1)$$

# Fields

A triple $(\mathcal{X}, +, \cdot)$ with operations $+, \cdot : \mathcal{X} \times \mathcal{X} \to \mathcal{X}$ is called a *field* if the following conditions hold:

- $\mathcal{X}$ with operation "+" forms an Abelian group, i.e.,

  $\exists$ *neutral element* "0": $a + 0 = 0 + a = a$ for all $a \in \mathcal{X}$

  $\exists$ *inverse elements:* $a + (-a) = (-a) + a = 0$ for all $a \in \mathcal{X}$

  *Associativity:* $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathcal{X}$

  *Commutativity:* $a + b = b + a$ for all $a, b \in \mathcal{X}$

- $\mathcal{X} \setminus \{0\}$ with operation "$\cdot$" forms an Abelian group with neutral element "1".

- *Distributivity* holds:

$$(a + b) \cdot c = a \cdot c + b \cdot c \text{ for all } a, b, c \in \mathcal{X}$$

# Fields

Example GF(2): $\mathcal{X} = \{0, 1\}$

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Example GF(4): $\mathcal{X} = \{x_1, x_2, x_3, x_4\}$

| $+$ | $x_0$ | $x_1$ | $x_2$ | $x_3$ |
|---|---|---|---|---|
| $x_0$ | $x_0$ | $x_1$ | $x_2$ | $x_3$ |
| $x_1$ | $x_1$ | $x_0$ | $x_3$ | $x_2$ |
| $x_2$ | $x_2$ | $x_3$ | $x_0$ | $x_1$ |
| $x_3$ | $x_3$ | $x_2$ | $x_1$ | $x_0$ |

| $\cdot$ | $x_0$ | $x_1$ | $x_2$ | $x_3$ |
|---|---|---|---|---|
| $x_0$ | $x_0$ | $x_0$ | $x_0$ | $x_0$ |
| $x_1$ | $x_0$ | $x_1$ | $x_2$ | $x_3$ |
| $x_2$ | $x_0$ | $x_2$ | $x_3$ | $x_1$ |
| $x_3$ | $x_0$ | $x_3$ | $x_1$ | $x_2$ |

Theorem. There exists a finite field of order $m$ if and only if $m = p^t$ for some prime $p$ and power $t \in \mathbb{N}$.

Construction by polynomials over GF(p).

# AES - Encryption

Most computations are in the field

$$\begin{aligned} F_{2^8} &= GF(2^8) \\ &= \{b_7x^7 + b_6x^6 + \cdots + b_1x + b_0 \mid b_i \in GF(2)\} \\ &= \{(b_7, b_6, \ldots, b_1, b_0) \mid b_i \in GF(2)\} \end{aligned}$$

Set of polynomials with coefficients from $F_2 = GF(2)$.

Addition:

Addition of polynomial coefficients.

Multiplication:

Multiplication of polynomials and taking the remainder modulo $q(x) = (x^8 + x^4 + x^3 + x + 1)$.