5.1.1. Key Generation

Key length 56 bits + 8 bits (parity check bits) (for error detection)

$K_0 = (k_{1,1}, \dots, k_{7,1}, b_1, k_{1,2}, \dots, k_{7,2}, b_2, \dots, k_{1,8}, \dots, k_{7,8}, b_8)$

From K_0 16 subkeys are generated: $K_1, \dots, K_{16}$.

- Form two blocks of 28 bits each: C_0, D_0.
- Construct C_i, D_i from C_{i-1}, D_{i-1} by a cyclic left shift by s_i positions with

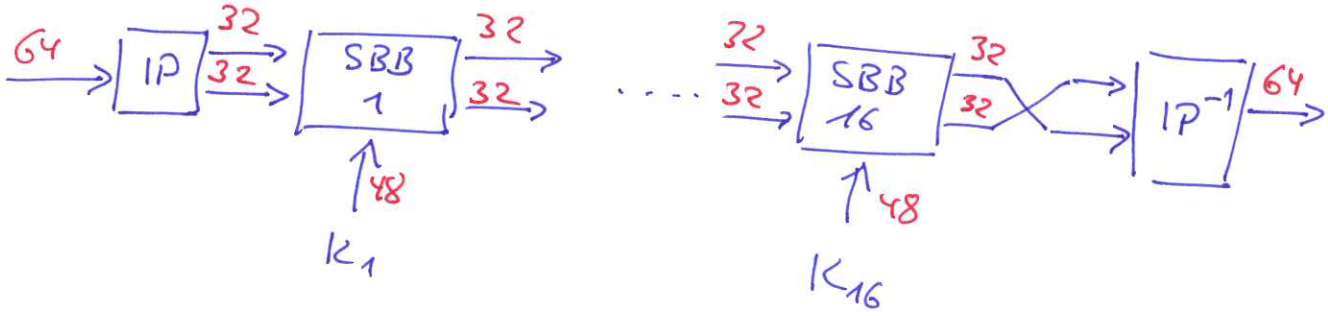
$$s_i = \begin{cases} 1, & \text{if } i \in \{1, 2, 9, 16\} \\ 2, & \text{otherwise} \end{cases}$$

- From each (C_i, D_i) select 48 bits.

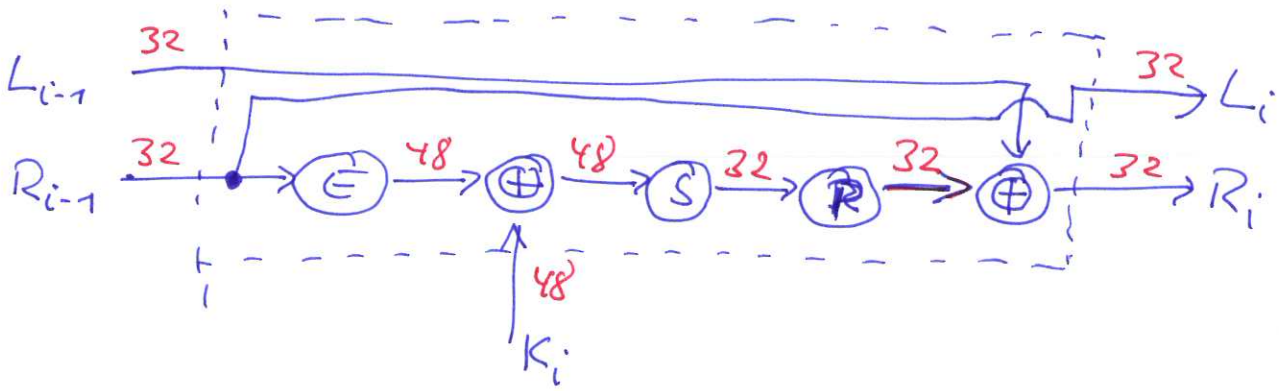
Each subkey is used in one standard building block (SBB).

5.1.2. DES Encryption

Plaintext m of 64 bits (otherwise group into blocks of 64 bits)



- IP (IP^{-1}) : initial permutation and its inverse, splitting into 2 blocks of 32 bits.
- SBB i : standard building block no. i



Formally: $L_i = R_{i-1}$

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

E : expansion map, permutation and doubling 16 bits.

$\oplus$: componentwise addition mod 2, xoring

P : permutation

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

48 bits are partitioned into 8 blocks of 6 bits each.

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

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

$a^{(i)}_{kl}$: (k,l)-th entry of S_i (S-Boxes)

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

Example:

$B_5 = (1\,0\,1\,0\,1\,0)$
$\wedge\ \vee\ \vee\ \vee\ \vee\ \wedge$

$\wedge$ $10 \hat{=} 2$

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

$a_{25}^{(5)} = 13 \hat{=} (1101)$ ⊥

5.1.3. DES Decryption

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

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

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

Hence, the same alg. can be used for decryption with keys $K_{16}, \dots, K_1$ in reverse order.

5.1.4. Security

Design criteria of the S-boxes are not fully published.

An IBM proposal was changed by the NSA.

Trapdoors? (non-confirmed rumor)

DES is vulnerable to essentially 2 attacks

- Differential cryptanalysis (Biham, Shamir CRYPTO 92) (Stinson, 02, p. 89 ff).
  S-boxes are optimized against diff. cryptanalysis.
  (Method was known to IBM researches 20 years ago?)
  Factor of 512 faster than exhaustive search.
- Exhaustive key search: (2^{56} key)

  1977: Diffie & Hellman proposed a machine,
  estimated US $ 20 million, could break DES in one day.

  1998: DES-cracker by Electronic Frontier Foundation
  US $ ~~€~~ 250.000, appr. 2 days.

  2006: COPACOBANA (Bochum, Kiel)
  120 FPGAs, $ 10.000, 6.4 days for cracking

  2008: COPACOBANA RIVYERA
  less than one day.

Main criticism: key of 56 bits is too short.

5.1.5. Triple-DES

Apply DES three times with different keys. 2 variants.

Key (K_1, K_2, K_3) (168 bits)

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

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 by $K_1 = K_2 = K_3$.

5.2 The Advanced Encryption Standard (AES)

Sept. 1997: NIST put out a call for replacement of DES.

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

Deadline of submission: June 98.

21 submitted proposals. After 3 AES-conferences

Rijndael (authors Daemen & Rijmen, Leuven, Belgium)

was chosen in a very open and fair competition.

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:

Computations 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))

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

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

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

Addition:

Addition of polynomial coefficients.

Multiplication:

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

Example:

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

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

$= y^9 + \cancel{y^8} + \cancel{y^6} + \cancel{y^4} + \cancel{y^2} + \cancel{y^8} + \cancel{y^7} + y^5 + y^3 + y +$

$\cancel{y^2} + \cancel{y^6} + \cancel{y^4} + \cancel{y^2} + 1$

$\cancel{6}\; y^9 + y^5 + y^3 + y + 1 : y^8 + y^4 + y^3 + y + 1 = y$

$y^9 + y^5 + y^4 + y^2 + y$

$1 \quad 1 \qquad y^4 + y^3 + y^2 + 1$

$\hat{=} (0\,0\,0\,1\,1\,1\,0\,1)$