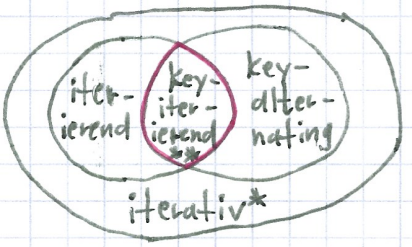
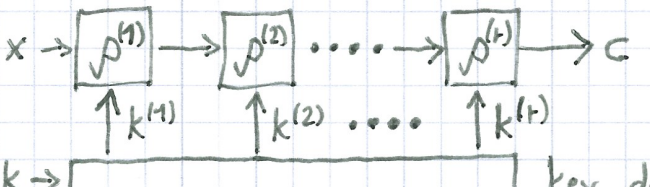
CRYPTO2-Übersicht: VL03: Klassifikation (DES) v. Blockchiffren; Int. von $\mathbb{B}^8$/Bytes

Klassif. v. Blockchiffren:

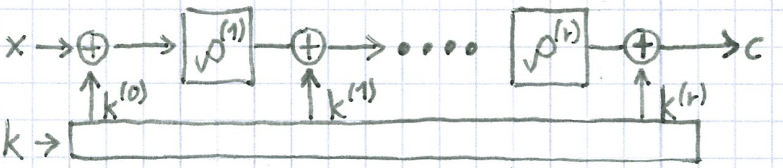


* auch: „rundenbasiert"
↳ heutzutage alle Blockchiffren!
** = AES (also die einfachste Bauart überhaupt!)

- **iterativ/„rundenbasiert"**: ρ: Rundentransformation

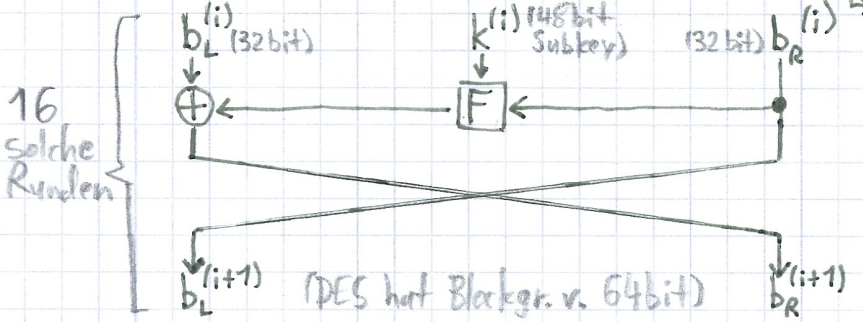


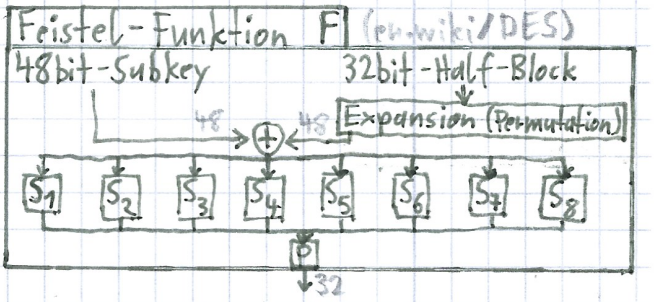
- **iterierend**: $\rho^{(2)} = \ldots = \rho^{(r-1)}$ ← AES ist beides! (sog. „key-iterierend")
- **key-alternating**:



Vorgänger von AES: DES (Data Encryption Standard): (=iterierend)

↳ DES = (balanciertes) Feistel-Chiffre





„Einschub über Bytes" (d.h. $\mathbb{B}^8$) aus der VL: Verschiedene Interpretationen:

GF(n) = $\mathbb{F}_n$

(1) $\mathbb{B}^8 \leftrightarrow$ 8-dim. VR über GF(2): $(0,0,0,0,0,1,1,0)+(0,0,0,0,0,1,1,1)=(0,0,0,0,0,0,0,1)$ (BE:6; LE:96) (BE:7, LE:224) (BE:1; LE:128) (*)

(2) $\mathbb{B}^8 \leftrightarrow (\mathbb{Z}_{256}, +)$: $(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )+(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )=(0,0,0,0,1,1,0,1)$ (BE:13)

↑ hier macht BE/LE einen Unterschied!

(25 ∈ℙ!) (3) $\mathbb{B}^8 \leftrightarrow (\mathbb{Z}_{257}^*, \cdot)$: $(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )\cdot(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )=(0,0,1,0,1,0,1,0)$ (BE:42)

0,..,0 → 1,..,1 (laut VL) / 1,0,0,...,0 ($t^0\ t^1\ t^2\ t^3\ t^4\ t^5\ t^6\ t^7$)

(4) $\mathbb{B}^8 \leftrightarrow GF(2^8) \leftrightarrow \mathbb{F}_2[t]/\langle R(t)\rangle$: $(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )+(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )=(0,0,0,0,0,0,0,1)$ (BE:1; LE:128) (*)

$(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )\cdot(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )=(0,1,0,1,0,0,0,0)$ (BE:80; LE:10)

Rechne stets modulo Rijndael-Polynom (irreduzibles) $R(t)=t^8+t^4+t+1$

$t^8+1 = t^8-1 \Leftrightarrow t^8=1$

(5) $\mathbb{B}^8 \leftrightarrow \mathbb{F}_2[t]/\langle t^8+1\rangle$: $(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )+(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )=(0,0,0,0,0,0,0,1)$ (BE:1; LE:128) (*)

$(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )\cdot(\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ )=(0,0,1,0,0,1,0,0)$ (BE:36; LE:36)

Bem.: (*) Addition im Polynomring entspricht Addition im VR! Dabei ist natürlich egal, ob Big- oder Little-Endian)

Truncated Polynomial Ring/„abgeschnittener Polynomring": Das Rechnen ist simpel ($t^8=1$):

$(t^6+1)\cdot(t^2+1) = t^8+t^6+t^2+1 = 1+t^6+t^2+1 = t^6+t^2$

$(t^7+1)\cdot(t^2+1) = t^9+t^7+t^2+1 = t+t^7+t^2+1 = t^7+t^2+t+1$

Sage:
(1) vector(GF(2), [0,1,1,0]) + vector(GF(2), [0,1,1,1]) → (0, 0, 0, 1)
(2) Zmod(256)(6) + Zmod(256)(7) == 13
(3) Zmod(257)(6) * Zmod(257)(7) == 42
(4) R = PolynomialRing(GF(2), t).quotient_ring(t^8 + t^4 + t + 1); R(...)
(5) R = PolynomialRing(GF(2), t).quotient_ring(t^8 + 1); R(t^9 + ...)