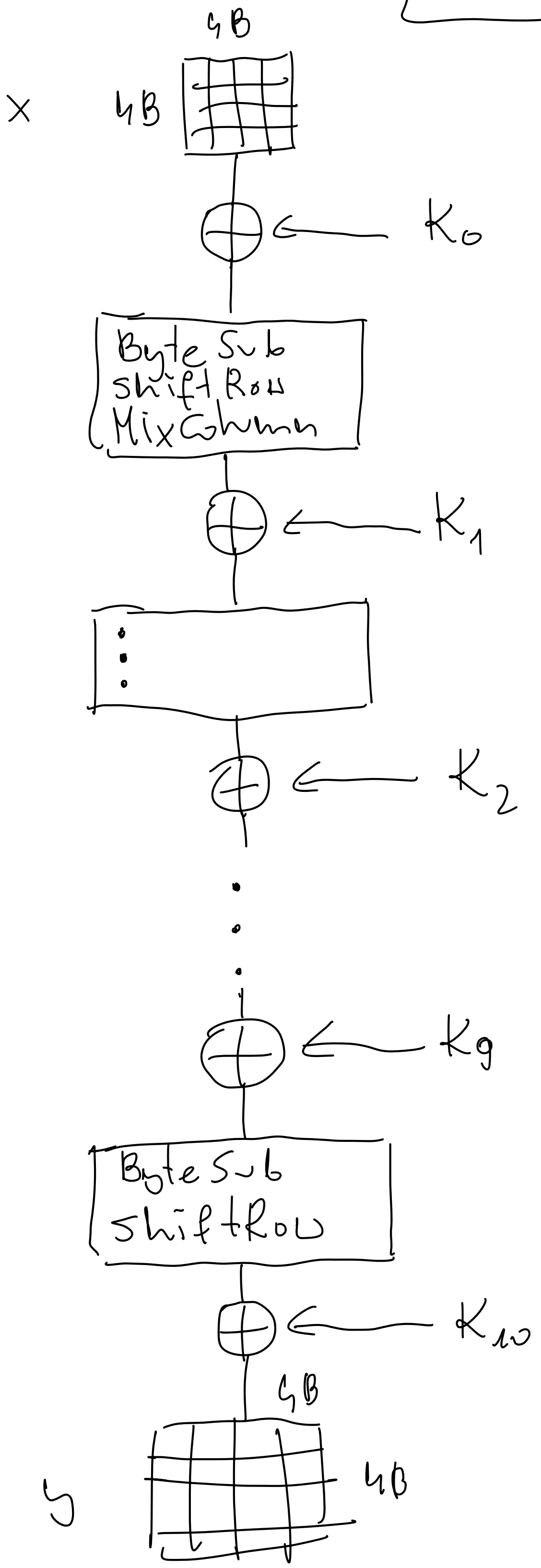
AES

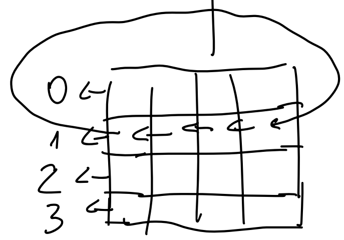
128 b   10 rund



→ ByteSub

ShiftRow

→ MixColumn



$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ $\qquad x \equiv y \pmod{n}$

$5 \cdot 7 = 15 \quad (\text{w } \mathbb{Z}_{20})$

$(\mathbb{Z}_n, +_n)$

grupa

- $+_n$ jest przemienne
- $+_n$ jest łączne $(a +_n b) +_n c_n = a +_n (b +_n c)$
- $+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$
- każdy el. $x \in \mathbb{Z}_n$ ma el. przeciwny, to znaczy istnieje $y \in \mathbb{Z}_n$, dla którego $x +_n y = 0$.

$\{ y = -x \quad , \quad y = -x = n - x \}$

$5 +_{20} \underbrace{(15)}_{-5} = 0$

$(\mathbb{Z}_n, \cdot_n)$

- $\cdot_n$ jest przemienne i łączne
- $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$
- 0 nie ma el. odw.

$\mathbb{Z}_{20} \quad 5^{-1} \quad y? \quad 5 \cdot_{20} y = 1$

$NWD(5, 20) = 5$

5^{-1} nie istnieje w $\mathbb{Z}_{20}$

$\mathbb{Z}_{20} \quad 3 \quad NWD(3, 20) = 1$

$3 \cdot 7 = 21 \equiv 1 \pmod{20}$

$3^{-1} = 7 \quad (\text{w } \mathbb{Z}_{20})$

$\boxed{RAI}$

Jeżeli $n = p$ jest liczbą pierwszą, to wszystkie el. $\mathbb{Z}_p$ są odwracalne.

$(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ ← grupa

$(\mathbb{Z}_p, +_p, \cdot_p)$ ← ciało (field)

$GF(2^8) \neq \{0, 1, \dots, 255\}$

↑

Galois field $\qquad GF(2^8) = \mathbb{F}_{2^8} \neq \mathbb{Z}_{2^8}$

$\mathbb{Z}_2 = \{0, 1\} \qquad (\mathbb{Z}_2, +_2, \cdot_2)$

$\mathbb{Z}_2[x]$ ← zbiór wielomianów o współczynnikach z $\mathbb{Z}_2$.

$x^2+1, \quad x^{10^{100}} + x^{2025} + x + 1, \quad \dots$

$x^8 + x^4 + x^3 + x + 1 \neq f(x) \cdot g(x)$

$f, g \in \mathbb{Z}_2[x]$

$f = 1 \lor g = 1$

$\mathbb{Z}_2[x] / x^8 + x^4 + x^3 + x + 1$

$$\boxed{\begin{gathered}\frac{f(x)}{g(x)} \\ f(x) = q(x) \cdot g(x) + r(x)\end{gathered}}$$

$$f \equiv g \pmod{x^8+x^4+x^3+x+1}$$

$$\iff x^8+x^4+x^3+x+1 \mid f(x)-g(x)$$

dzieli

$$\#\left(\underbrace{\mathbb{Z}_2[x]/x^8+x^4+x^3+x+1}\right) = 2^8$$

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

$$\underbrace{\overbrace{b_7 b_6 \ldots b_0}^{\{0,1\}}} \qquad 2^8$$

$$(\mathbb{F}_{2^8}, +, \cdot)$$

$$\{b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x+b_0\}$$

$$f, g \in \mathbb{F}_{2^8} \qquad f+g \qquad b_i \in \{0,1\}$$

$$f \cdot g$$

$$(x^5+x^4+x)+(x^6+x^2+x+1) = x^6+x^5+x^4+x^2+2x+1$$

$$= x^6+x^5+x^4+x^2+1$$

$$\{\underbrace{0011}\underbrace{0010}\}_2 \oplus \{01000111\}_2 = \{01110101\}_2$$

$$\{32\}_{16} \oplus \{47\}_{16} = \{75\}_{16}$$

$f \in \mathbb{F}_{2^8}$ $\qquad f \cdot g$

$f \cdot x$

$f(x) = b_7 x^7 + b_6 x^6 + \ldots + b_1 x + b_0 = \{b_7 b_6 \ldots b_0\}$

$f(x) \cdot x = \underbrace{b_7 x^8 + b_6 x^7 + \ldots + b_1 x^2 + b_0 x}$

$$\underbrace{\{b_7 \ldots b_1 b_0\}}_{f} \cdot \underbrace{\{00000010\}}_{x} = \begin{cases} \{b_6 b_5 b_4 b_3 b_2 b_1 0\} & b_7 = 0 \\ \{b_6 b_5 b_4 (b_3+1)(b_2+1) b_1 b_0 1\} & b_7 = 1 \end{cases}$$

$f(x) \cdot x = x^8 + b_6 x^7 + b_5 x^6 + \ldots + b_1 x^2 + b_0 x : \underline{x^8 + x^4 + x^3 + x + 1} = 1$

$+ \quad x^8 + x^4 + x^3 + x + 1$

$= \underbrace{b_6 x^7 + b_5 x^6 + b_4 x^5 + (b_3+1) x^4 + (b_2+1) x^3 + b_1 x^2 + (b_0+1) x + 1}$

$f(x) \cdot (x^4 + x + 1) = \underbrace{f(x) \cdot x^4} + f(x) \cdot x + f(x)$

$(((f(x) \cdot x) \cdot x) \cdot x) \cdot x$

$(\mathbb{F}_{2^8}, +, \cdot)$ jest ciało

ByteSub $(f = \{b_7 b_6 \ldots b_1 b_0\})$

if $f \neq 0$:

$\boxed{f \leftarrow f^{-1}}$ $\leftarrow$ RAE

$c = \{01100011\}$

$\{g = \{a_7 a_6 \ldots a_1 a_0\}\}$

for i in $0..7$: $\qquad$ indeksy mod 8

$a_i = (b_i + b_{i+4} + b_{i+5} + b_{i+6} + b_{i+7} + c_i) \bmod 2$

return $\{a_7 a_6 \ldots a_1 a_0\}$