$$(x^6+x^4+x+1)^{-1} = ?$$ u $\mathbb{F}_{2^8}$ $\quad \mathrm{NHD}(a,b) = \mathrm{NHD}(b, a \bmod b)$

$$x^8+x^4+x^3+x+1 : x^6+x^4+x+1 = x^2+1$$
$$+\ x^8+x^6+x^3+x^2$$
$$= x^6+x^4+x^2+x+1$$
$$+\ x^6+x^4+x+1$$
$$= \quad = x^2$$

$$x^8+x^4+x^3+x+1 = (x^2+1)\underbrace{(x^6+x^4+x+1)} + \underbrace{x^2}$$

$$x^6+x^4+x+1 : x^2 = x^4+x^2$$
$$+\ x^6$$
$$= x^4+x+1$$
$$x^4$$
$$= x+1$$

$$x^6+x^4+x+1 = (x^4+x^2)\underbrace{x^2} + \underbrace{x+1}$$

$$x^2 : x+1 = x+1$$
$$+\ x^2+x$$
$$= x$$
$$+\ x+1$$
$$1$$

$$\underbrace{x^2 = (x+1)(x+1)+1}$$

$$1 = x^2 - (x+1)(x+1) = x^2 - \left(x^6+x^4+x+1-(x^4+x^2)x^2\right)(x+1)$$
$$= (x^6+x^4+x+1)(x+1) + x^2 + x^2(x^4+x^2)(x+1) =$$
$$= (x^6+x^4+x+1)(x+1) + x^2(1+x^5+x^4+x^3+x^2) =$$
$$= (x^6+x^4+x+1)(x+1) + x^2(x^5+x^4+x^3+x^2+1)$$
$$= (x^6+x^4+x+1)(x+1) + \left[x^8+x^4+x^3+x+1 + (x^6+x^4+x+1)(x^2+1)\right]$$
$$(x^5+x^4+x^3+x^2+1)$$

$$= (x^8 + x^4 + x^3 + x + 1)(x^5 + x^3 + \dots + 1)$$

$$+ (x^6 + x^4 + x + 1)\Big[\underbrace{x + 1 + (x^2+1)(x^5 + x^4 + x^3 + x^2 + 1)}\Big]$$

$$x + \cancel{1} + x^7 + x^6 + \cancel{x^5} + \cancel{x^4} + \cancel{x^2} + \cancel{x^5} + \cancel{x^4} + x^3 + \cancel{x^2} + \cancel{1} =$$

$$= x^7 + x^6 + x^3 + x$$

$$1 = (x^8 + \dots)(\dots) + (x^6 + x^4 + x + 1)(x^7 + x^6 + x^3 + x)$$

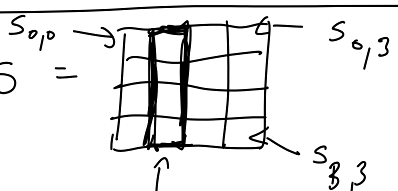
$$\Big| \bmod x^8 + \dots$$

$$1 = (x^6 + \dots)(x^7 + x^6 + x^3 + x) \quad \text{in } \mathbb{F}_{2^8}$$

$$(x^6 + x^4 + x + 1)^{-1} = x^7 + x^6 + x^3 + x \quad \text{in } \mathbb{F}_{2^8}$$

$$\underset{f}{(01010011)^{-1}} = \underset{f^{-1}}{11001010}$$

MixColumn

$S =$ 

$$\begin{bmatrix} s_{0,j} \\ s_{1,j} \\ s_{2,j} \\ s_{3,j} \end{bmatrix} \rightsquigarrow \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{bmatrix}$$

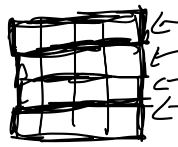
$$u_0 = x\, s_{0,j} + (x+1)\, s_{1,j} + s_{2,j} + s_{3,j}$$

$$u_1 = x\, s_{1,j} + (x+1)\, s_{2,j} + s_{3,j} + s_{0,j}$$

$u_2 = x\, s_{2,j} + (x+1)\, s_{3,j} + x_{0,j} + x_{1,j}$

$u_3 = x\, s_{3,j} + (x+1)\, s_{0,j} + s_{1,j} + s_{2,j}$

KeyExpansion $\underset{128b}{K} \rightsquigarrow \underbrace{K_0, K_1, \dots, K_{10}}_{128b}$

$K =$ 

Rcon (round constant)

$rcon_1$	=	01	00 00 00
$rcon_2$	=	02	00 00 00
$rcon_3$	=	04	00 00 00
4		08	...
5		10	...
6		20	...
7		40	...
8		80	...
9		1B	...
10		36	...

4B

0

KeyExpansion

IN: K 128b

OUT: $\boxed{K_0, K_1, \dots, K_{10}}$ $\quad 11 \cdot 16B$

$11 \cdot 4 \cdot 4B$

$44 \cdot 4B$

$w_0, w_1, \dots, w_{43} \leftarrow 4B$

$i: 0..3:$

$\quad w_i \leftarrow (k_{4i}, k_{4i+1}, k_{4i+2}, k_{4i+3})$

$i: 4..43:$

$\quad tmp \leftarrow w_{i-1}$

$\quad$ if $i \% 4 = 0:$

$\quad\quad tmp \leftarrow \underline{SubWord}(\underline{ShiftWord}(tmp)) \oplus rcon_{i/4}$

$\quad w_i \leftarrow w_{i-1} \oplus tmp$

return $w_0, w_1, \dots, w_{43}$

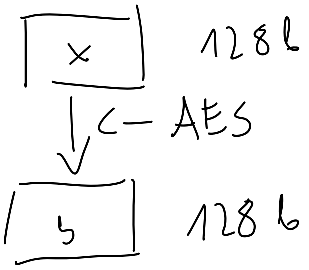
$ShiftWord(\underbrace{v_0, v_1, v_2, v_3}_{4B}) =$

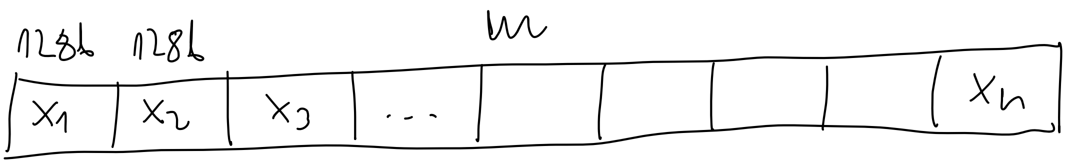
$= (v_1, v_2, v_3, v_0)$

$SubWord(v_0, v_1, v_2, v_3) =$

$= (SBox(v_0), Sbox(v_1), Sbox(v_2), Sbox(v_3))$

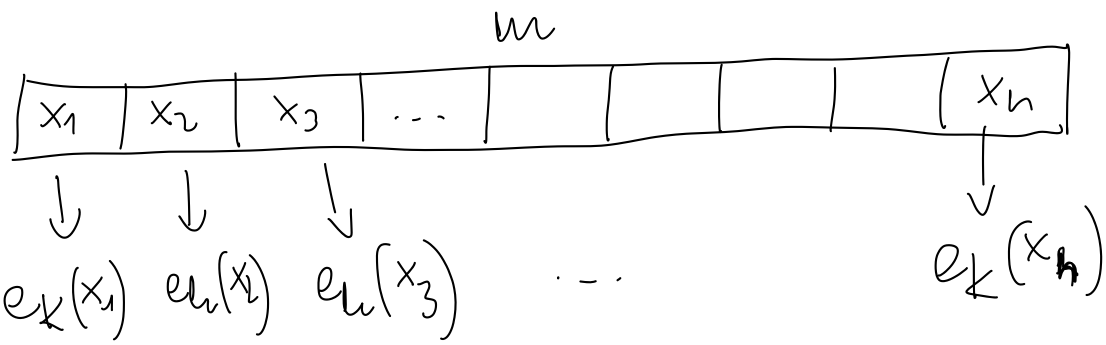
AES





Tryby:

- ECB — electronic codebook (NIE STOSOWAĆ)
- CBC — cipher block chaining
- OFB — output feedback
- CFB — cipher feedback
- CTR — counter



CBC