

MAC336 (cripto)

(102)

Propriedade do DES

$$\overline{\text{DES}_k(x)} = \text{DES}_k(x) = \text{fraqueza conhecida}$$

$$y = \text{DES}_k(x)$$

↳ desconhecido  $2^{56}$  universo

Como propriedade,  $U = 2^{55}$

AES

Opér sobre bytes (8 bits)

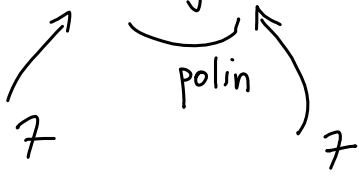
(1) soma e xor  $\oplus$

subtraç // //

(2) multiplicação

$$f(x) \cdot g(x) \text{ mod } (x^8 + x^4 + x^3 + x + 1)$$

$m(x)$



grau  
↳ 7  
no máx

Sendo  $m(x)$  primo, cada byte  $b(x)$  possui um inverso  $b^{-1}(x) \text{ mod } m(x)$  tal que (apaga a lousa)  $\rightarrow$  seja bijetora