Propriedade do DES

$\overline{DES_{\overline{K}}(\overline{x})} = DES_K(x)$ ⇒ fraqueza

$y = DES_k(x)$ — x conhecido

↳ desconhecido 2^{56} universo

Com a propriedade, $U = 2^{55}$

AES

Opr sobre bytes (8 bits)

(1) soma é xor ⊕

subtração // //

(2) multiplicação

$f(x) \cdot g(x) \bmod (x^8 + x^4 + x^3 + x + 1)$ — $m(x)$ — grau 7 no máx

$f(x)$ — polin — $g(x)$

Sendo $m(x)$ primo, cada byte $b(x)$ possui um inverso $b^{-1}(x) \bmod m(x)$ tal que (apagou aluna) ↳ rija bijetora