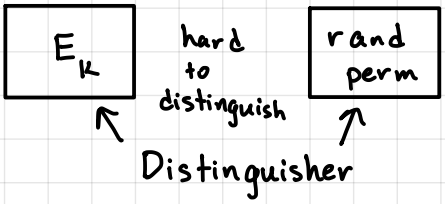
Block cipher is intended to resemble a random permutation



Byte Substitution:

$$S(x) = x^{-1} \cdot C_1 + C_2$$

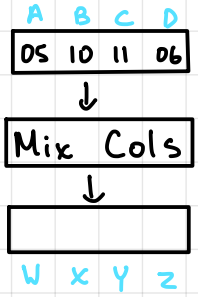
affine cipher

over $GF(2^8)$

$02 \cdot B$ ← 0x03

00000010 00000011

$x \cdot (x+1) = x^2 + x = 00000110$



10 = 10000 11 = 10001

05 = 101 06 = 0110

$w = 2 \cdot A + 3 \cdot B + 1 \cdot C + 1 \cdot D$

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

$= (x^3+x) + (x^5+x^4) + (x^4+1) + (x^2+x)$

$= x^5 + x^3 + x^2 + 1$

$= 00101101$

$= 2D$