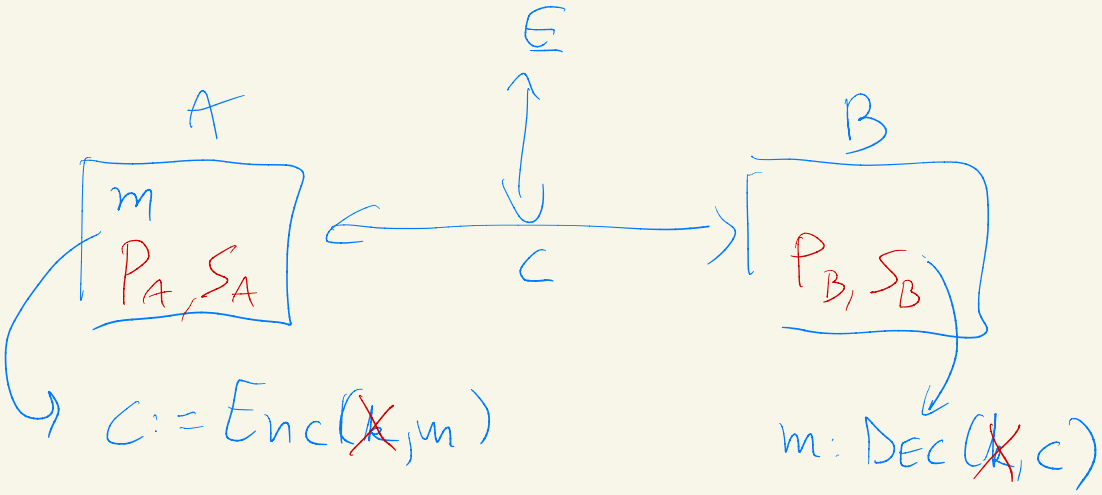

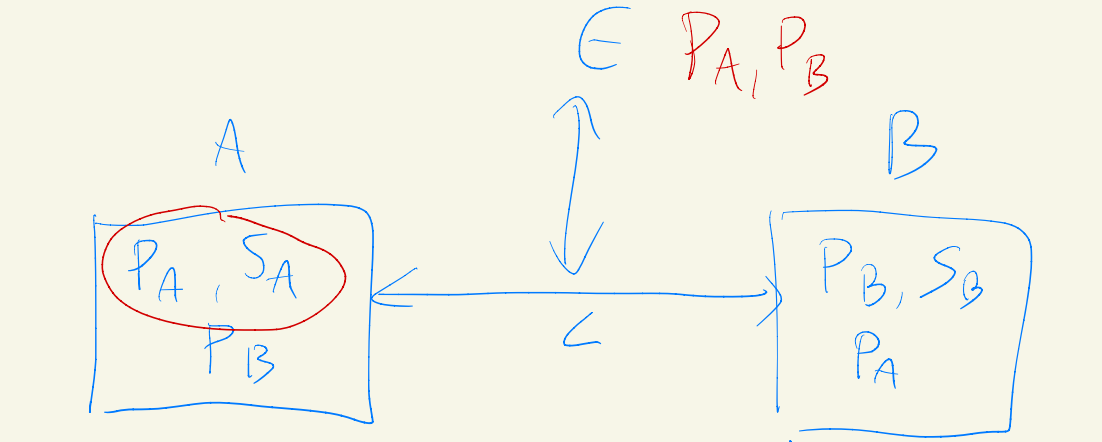

$C := Enc(P_B, m)$ P_B $m := Dec(S_B, c)$

$m := Dec(S_B, Enc(P_B, m))$

$a, b \in \mathbb{Z} \quad b \neq 0$

existen números α, β:

$$a = \alpha \cdot b + \beta$$

$$0 \leq \beta < |b|$$

además son únicos

$$a \bmod b = \beta$$

$13 = 1 \cdot 5 + \cancel{8}$

$13 \bmod 5 = 3$

$13 = 2 \cdot 5 + (3)$

$-10 \bmod -3 = 2$

$-10 = 4(-3) + \boxed{2}$

Def: $a \equiv b \bmod n$ ssi $n \mid (b - a)$

Prop: $a \equiv b \bmod n$ ssi $a \bmod n = b \bmod n$

mod 5 $\qquad\qquad$ $3 \equiv 8 \mod 5$

$5 \mid 8-3$

$3 \bmod 5 = 3 = 8 \bmod 5$

4, 5 $\qquad\qquad$ $0 \le B < 5$

$\{0, 1, 2, 3, 4\}$

Prop: $\quad a \equiv b \mod n$

$c \equiv d \mod n$

$\Rightarrow \quad (a+c) \equiv (b+d) \mod n$

$(a \cdot c) \equiv (b \cdot d) \mod n$]

Algoritmos básicos

MCD: máximo común divisor

n

$O(n)$

10^{400}

n

$\log_2 n$

$\log_2 n$

$O((\log_2 n)^k)$

$a \geq b$

$MCD(a, b)$

$O((\log_2 a)^2)$

MCD

MCD(a, b)

$a \geq b$

$a > 0$

$a = p_1^{s_1} \cdots p_\ell^{s_\ell}$

$b = p_1^{t_1} \cdots p_\ell^{t_\ell}$

$12 = 2^2 \cdot 3$

$14 = 2 \cdot 7$

$12 = 2^2 \; 3^1 \; 7^0$

$14 = 2^1 \; 3^0 \; 7^1$

$MCD(a,b) = p_1^{\min(s_1,t_1)} \cdots p_\ell^{\min(s_\ell,t_\ell)}$

$MCM(a,b) = p_1^{\max(s_1,t_1)} \cdots p_\ell^{\max(s_\ell,t_\ell)}$

$N \rightsquigarrow (P)$ $\quad \frac{N}{P}$

$12 \to 4 \to 2 \cdot 2$ $\quad \frac{12}{4}$

$$MCD(a,b) = \begin{cases} MCD(b, a \bmod b) & b > 0 \\ a & b = 0 \end{cases}$$

$a \geq b \geq 0$

$a \neq 0$

$MCD(5,0) = 5$

$MCD(14,12) = MCD(12,2)$

$= MCD(2,0)$

$= 2$

Prop: $a \geq b \geq 0 \quad a \neq 0$

$$a \bmod b < \frac{a}{2}$$