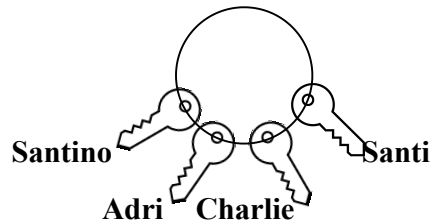


Colección de claves
públicas obtenidas por

Anto

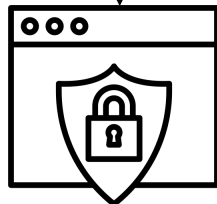


PR_b Clave privada de
Charlie

PU_b Clave pública de
Charlie

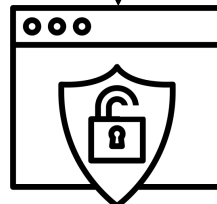


X



Texto cifrado
transmitido

$Y = E(PR_b, X)$



$X = D(PU_b, Y)$



Texto claro
de entrada

Algoritmo de
encriptado

Algoritmo de desencriptado
(Reversa del algoritmo
de encriptado)

Texto claro
de salida

Charlie

Anto