

Compute

$$C \equiv a^b \pmod{n}$$

for a given  $a \in \mathbb{Z}$ ,  $b, n \in \mathbb{N}$

$$C \equiv a^b = \underbrace{a \cdot a \cdot \dots \cdot a}_n \pmod{n}$$

IN:  $a \in \mathbb{Z}$ ,  $b, n \in \mathbb{N}$

OUT:  $c \in \mathbb{Z}$ ,  $c \equiv a^b \pmod{n}$

1.  $c \leftarrow 1$

2. for  $i \leftarrow 0$  to  $b-1$  do

3.  $c \leftarrow c \cdot a$

4.  $c \leftarrow c \pmod{n}$   $\rightarrow$  Euclidean



-||-

1.  $c \leftarrow 1$

2. for  $i \leftarrow 0$  to  $b-1$  do

3.  $c \leftarrow c \cdot a$

4.  $c \leftarrow c \pmod{n}$

$$2^{42} \equiv 4398046511104 \equiv 1 \pmod{127}$$

# Right-to-Left

1.  $c \leftarrow 1, t \leftarrow a$
2. for  $i=0$  to  $l-1$  do  
if  $b_i = 1$  then  
 $c \leftarrow c \cdot t \pmod n$   
 $t \leftarrow t^2 \pmod n$
3. return  $c$

$$42 = (101010)_2 =$$

$2^5 + 2^3 + 2^1$

$$l = 6$$

---

	$(c, t)$
	$(1, a)$ init
$i=0$	$(1, a^2)$ ( $b_0 = 0$ ; there is no $2^0$ )
$i=1$	$(a^2, a^4)$ ( $b_1 = 1$ ; there is $2^1$ )
$i=2$	$(a^2, a^8)$
$i=3$	$(a^{10}, a^{16})$
$i=4$	$(a^{10}, a^{32})$
$i=5$	$(a^{42}, a^{64})$

$\rightarrow a^{42}$

## Left-to-right

1.  $c \leftarrow 1$

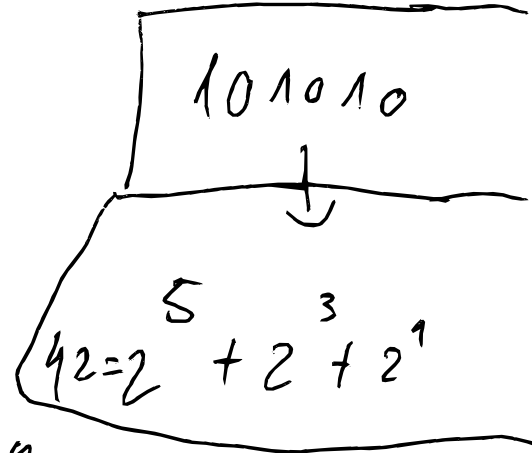
2. for  $i \leftarrow l-1$  to  $0$  do

$$c \leftarrow c^2 \pmod n$$

if  $b_i = 1$  then

$$c \leftarrow c \cdot a \pmod n$$

3. return  $c$



	(c)
init	1
$i=l-1$	$a$ ( $b_5 = 1$ )
$i=4$	$a^2$ ( $b_4 = 0$ )
$i=3$	$a^5$ ( $b_3 = 1$ )
$i=2$	$a^{10}$ ( $b_2 = 0$ )
$i=1$	$a^{21}$ ( $b_1 = 1$ )
$i=0$	$a^{42}$ ( $b_0 = 0$ )