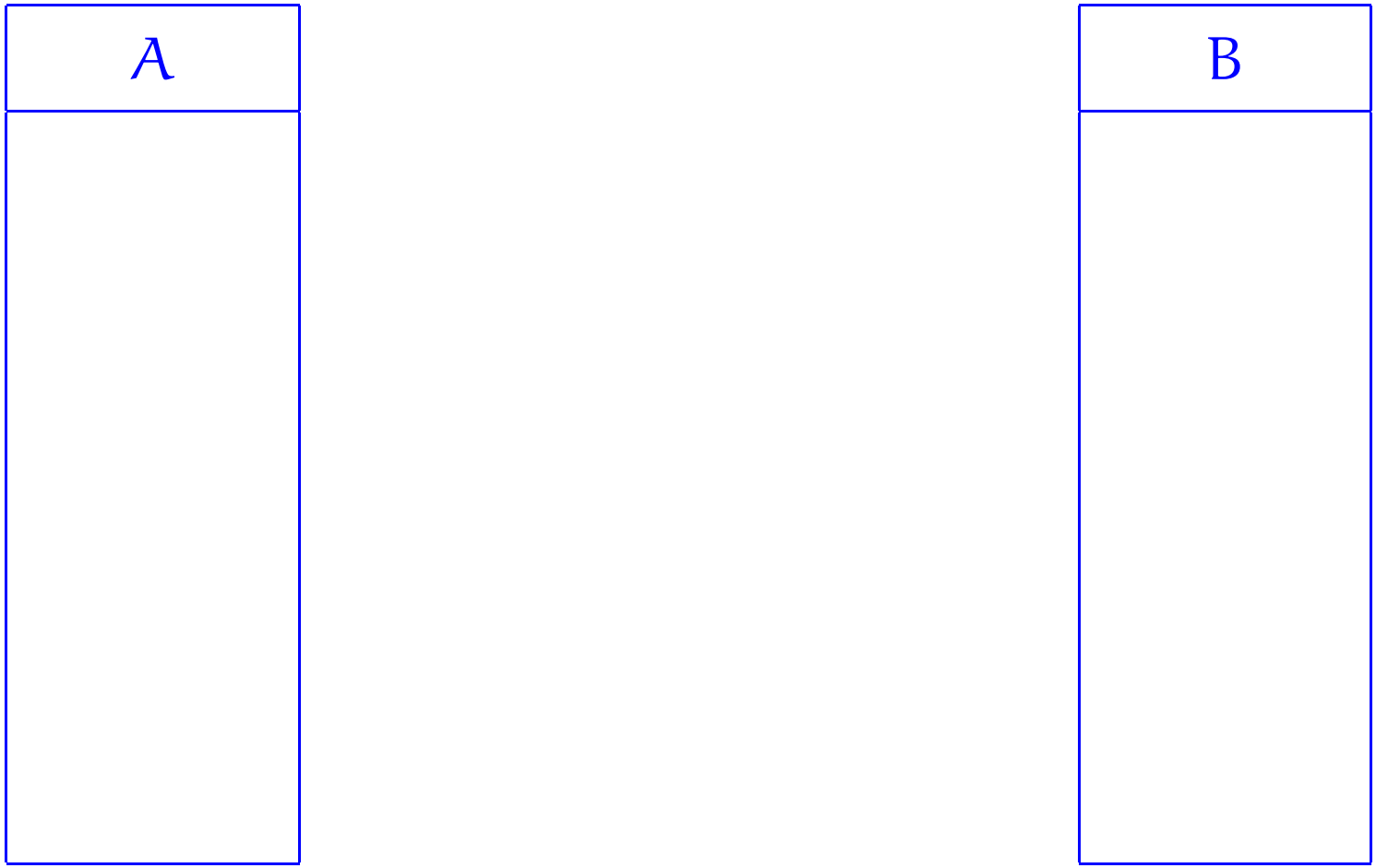
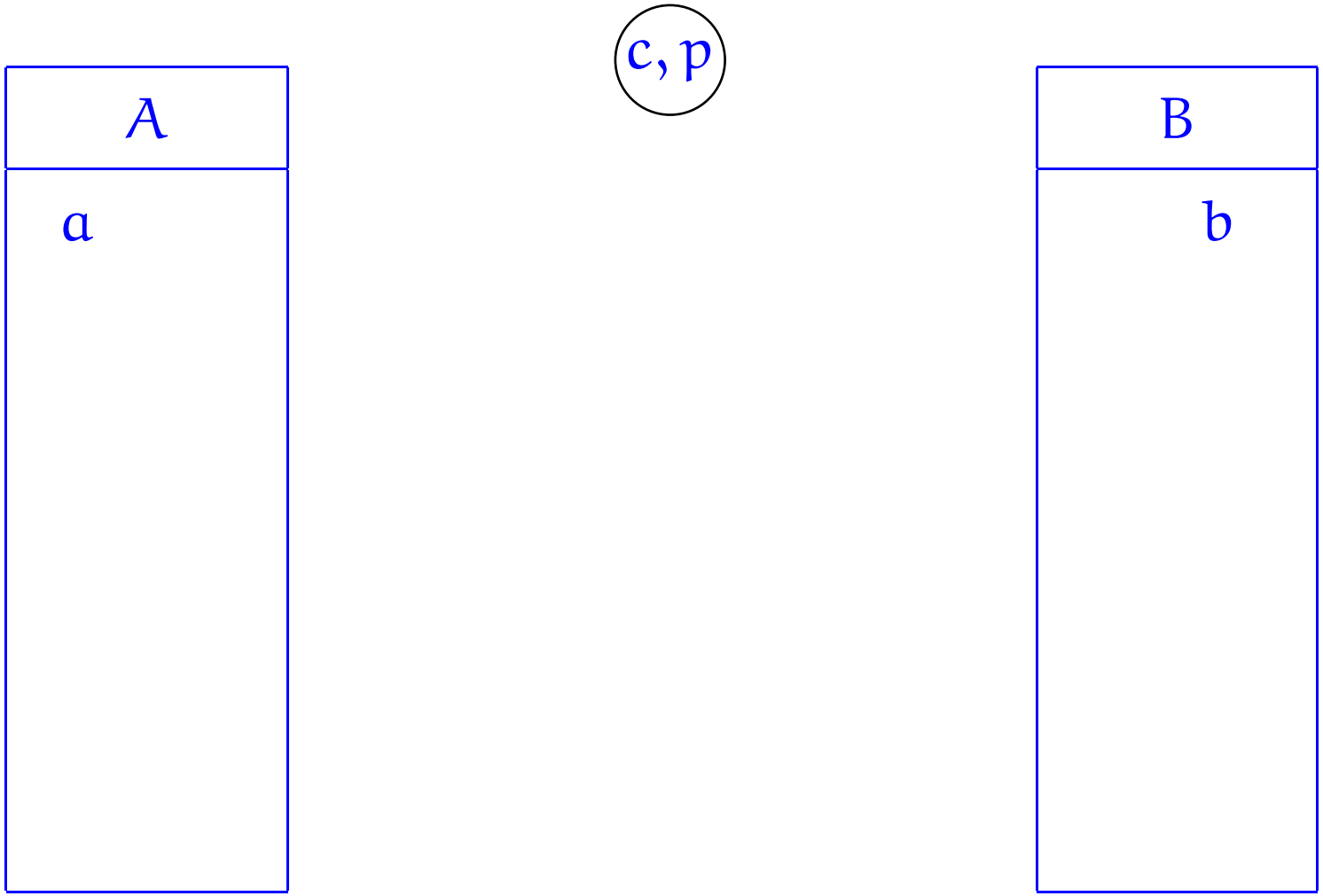
Diffie-Hellman cryptographic method

Shared secret key



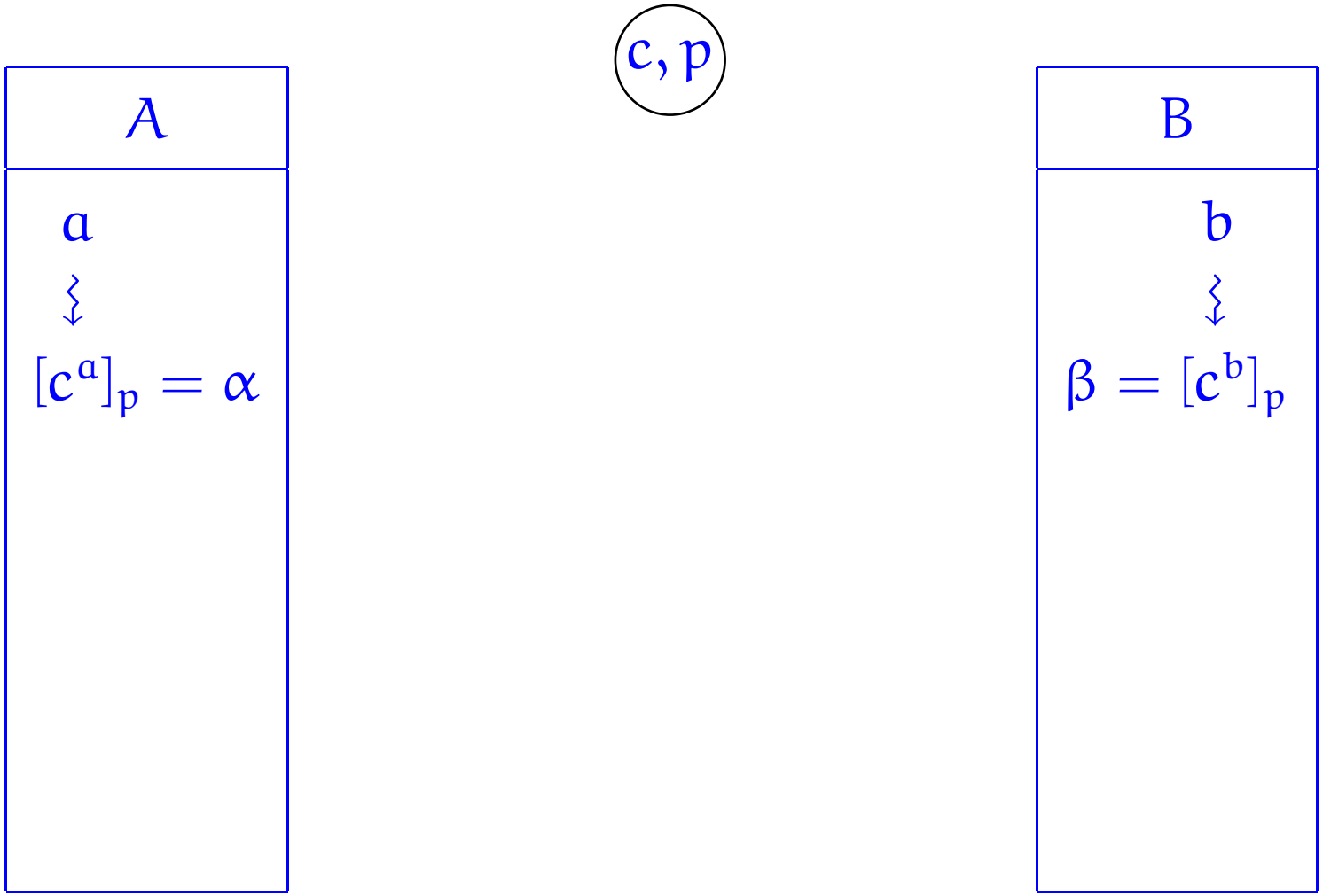
Diffie-Hellman cryptographic method

Shared secret key



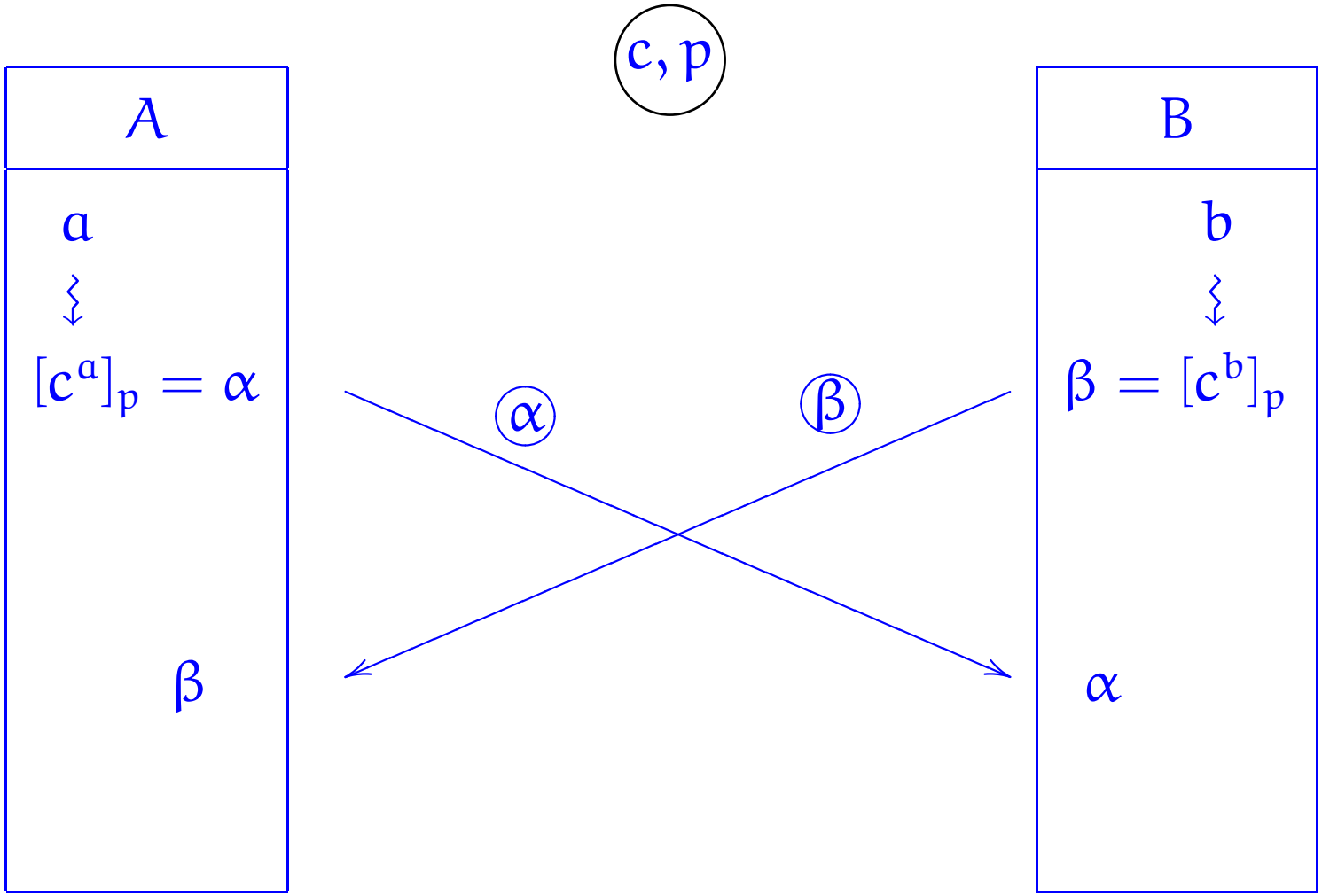
Diffie-Hellman cryptographic method

Shared secret key



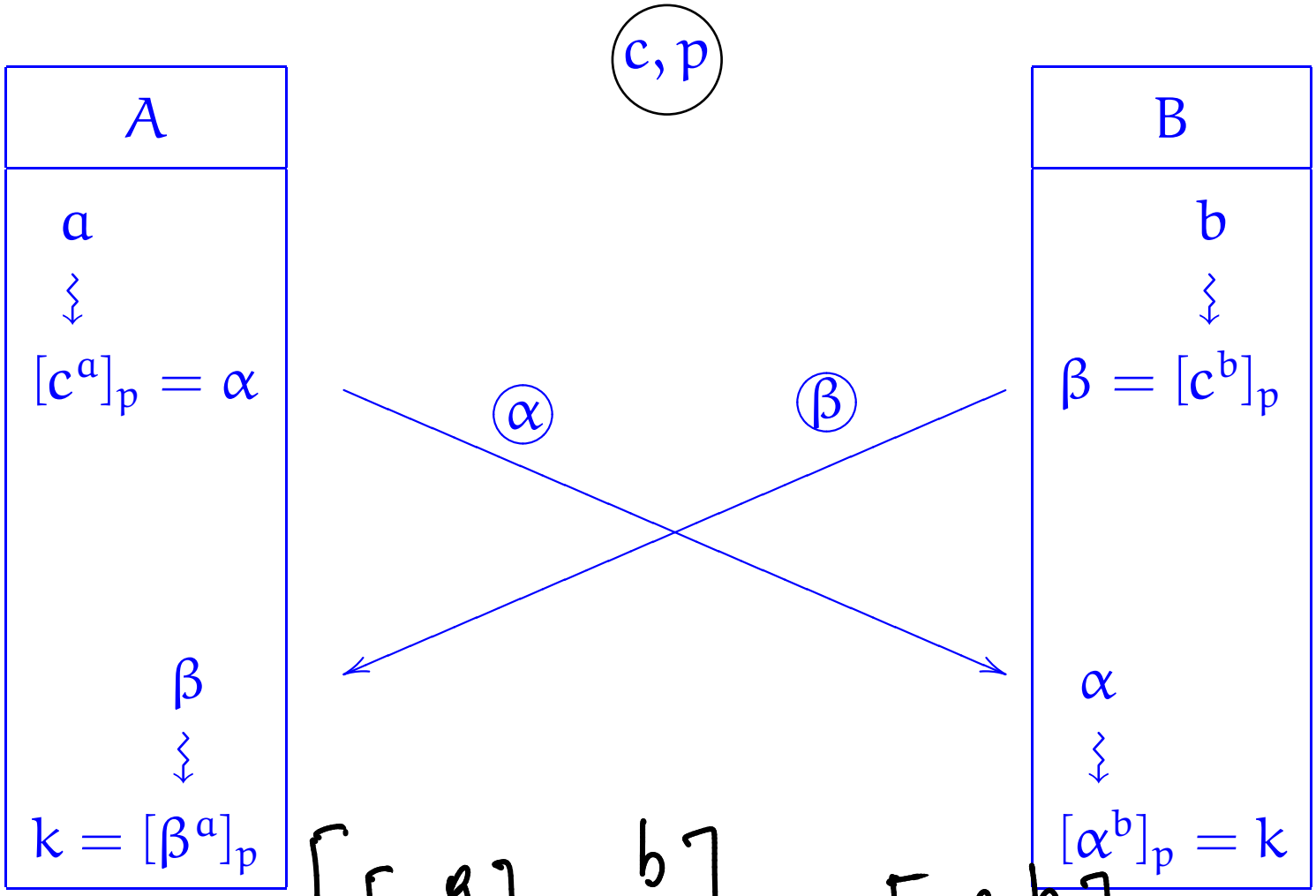
Diffie-Hellman cryptographic method

Shared secret key



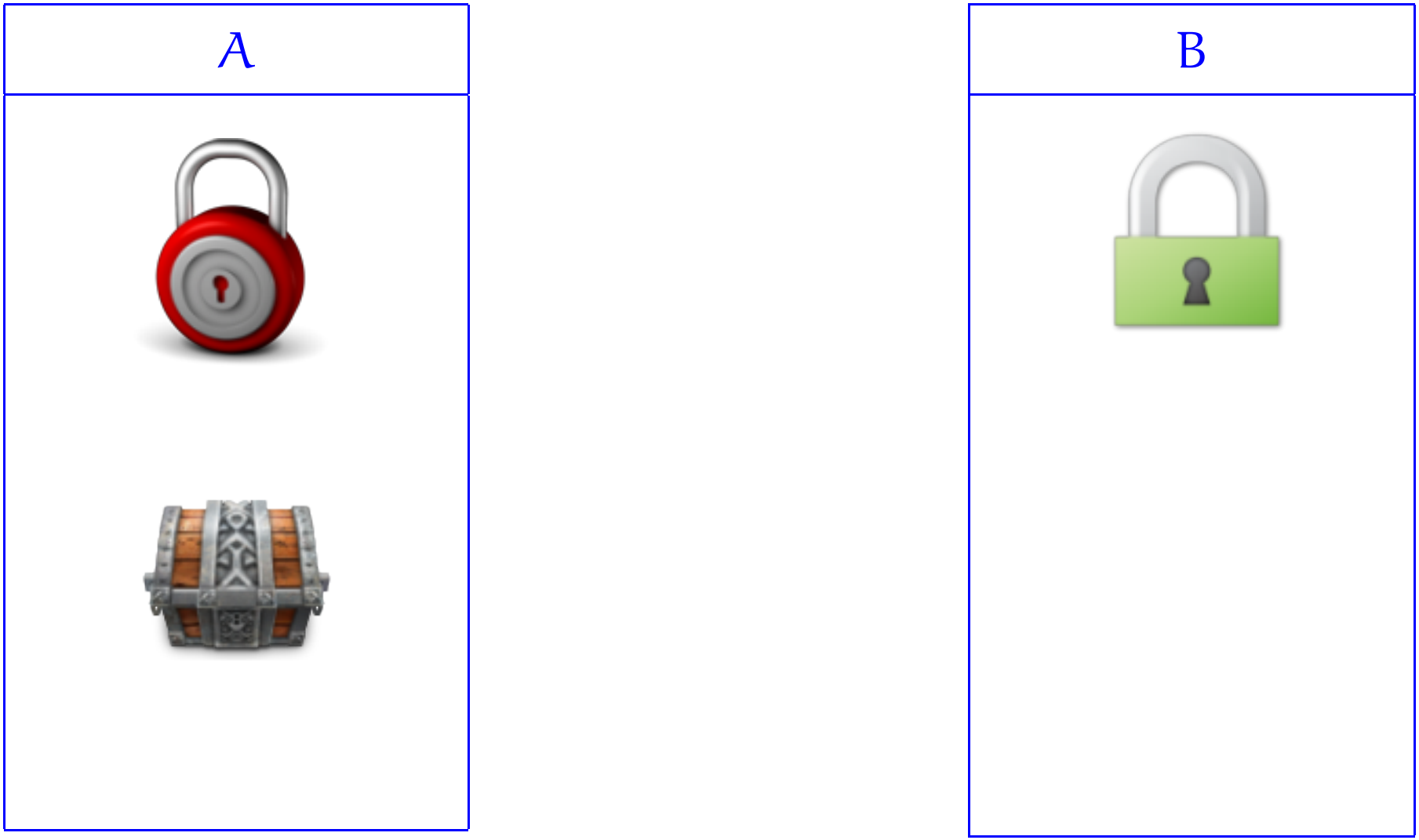
Diffie-Hellman cryptographic method

Shared secret key



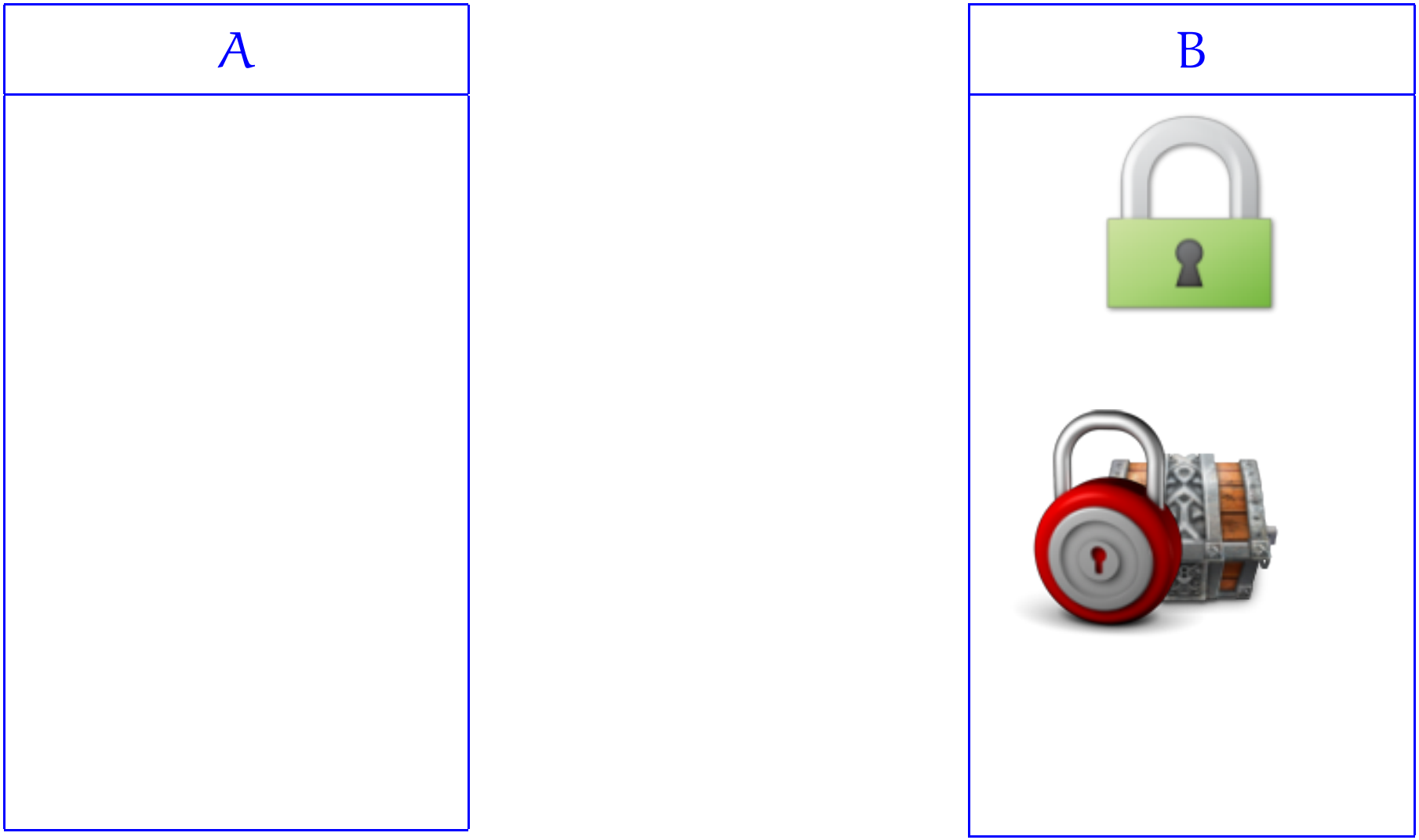
$$\left[[c^a]_p \quad ^b \right]_p = \left[c^{ab} \right]_p$$

Key Exchange



Key Exchange

Key Exchange



Key Exchange

A

B

Key Exchange

A

B

Key Exchange

A

B

Key Exchange

A

B

Key Exchange

Key exchange

Lemma 75 *Let* p *be a prime and* e *a positive integer with* $\gcd(p-1, e) = 1$. *Define*

$$d = \left[\mathrm{lc}_2(p-1, e) \right]_{p-1} .$$

Then, for all integers k,

$$(k^e)^d \equiv k \pmod{p} .$$

(efficiently computable)

PROOF: $\gcd(p-1, e) = 1 \Rightarrow \exists\, l_1, l_2 \in \mathbb{Z}.$

$$l_1 \cdot (p-1) + l_2 \cdot e = 1$$

Know $l_1, l_2 \in \mathbb{Z}$:

$$l_1(p-1) + l_2 \cdot e = 1$$

$$\Rightarrow \quad l_2 \cdot e \equiv 1 \pmod{p-1}$$

$$\Rightarrow \quad d \cdot e \equiv 1 \pmod{p-1} \quad d \overset{\text{def}}{=} [l_2]_{p-1}$$

(since $d \equiv l_2 \pmod{p-1}$)

$$\Rightarrow \quad d \cdot e - 1 = c \cdot (p-1) \text{ for some integer } c$$

$$\Rightarrow (k^e)^d = k^{de} = k^{c(p-1)+1} \overset{\text{positive}}{=} k \cdot \left(k^{(p-1)}\right)^c$$

$$\Rightarrow (k^e)^d \equiv k \cdot (k^{p-1})^c \pmod p$$

$$\equiv k \cdot 1^c \pmod p$$

FLT

$$= k$$

provided $k \not\equiv 0 \pmod p$

If $k \equiv 0 \pmod p$

Then $(k^e)^d \equiv k \equiv 0 \pmod p$

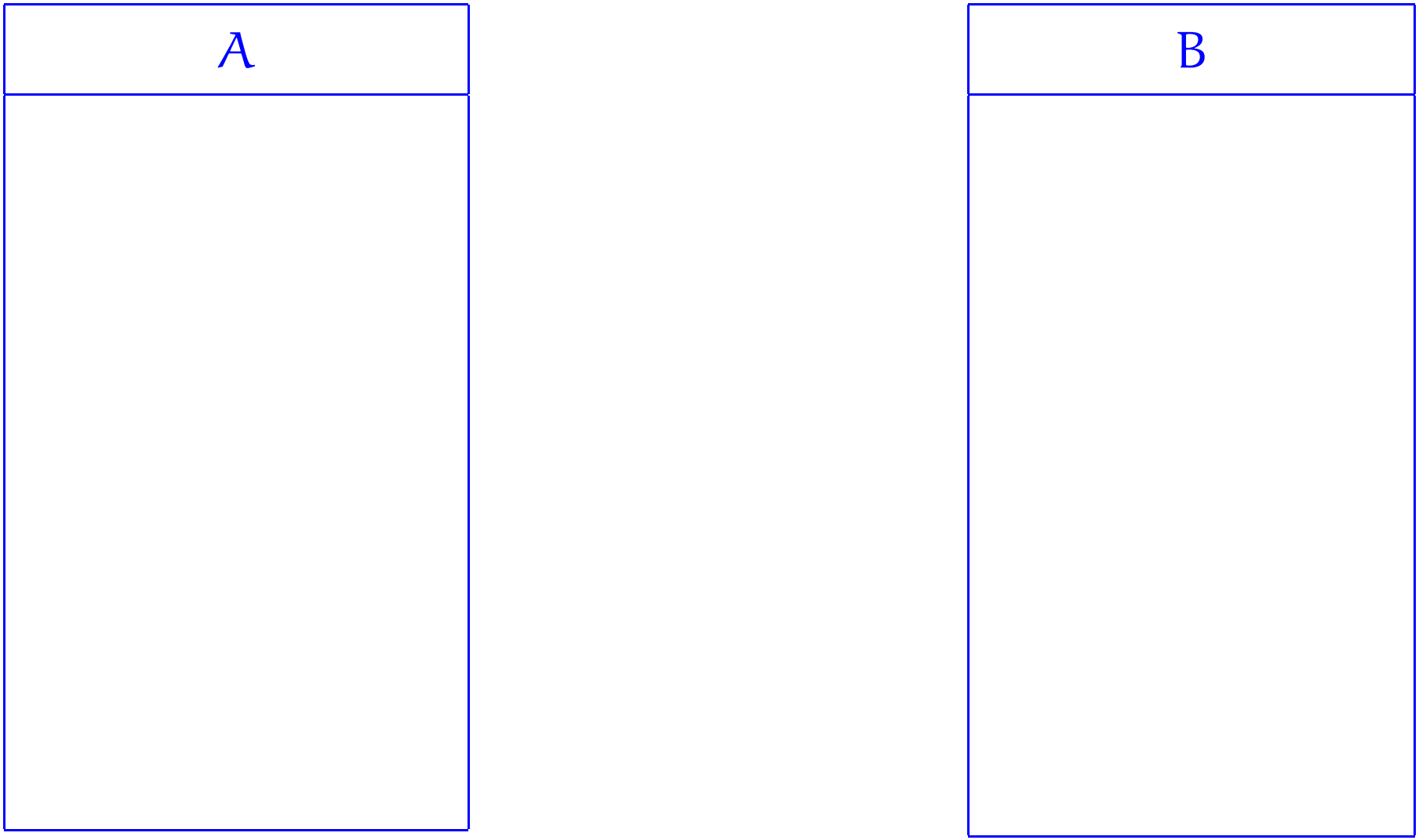
$\boxtimes$

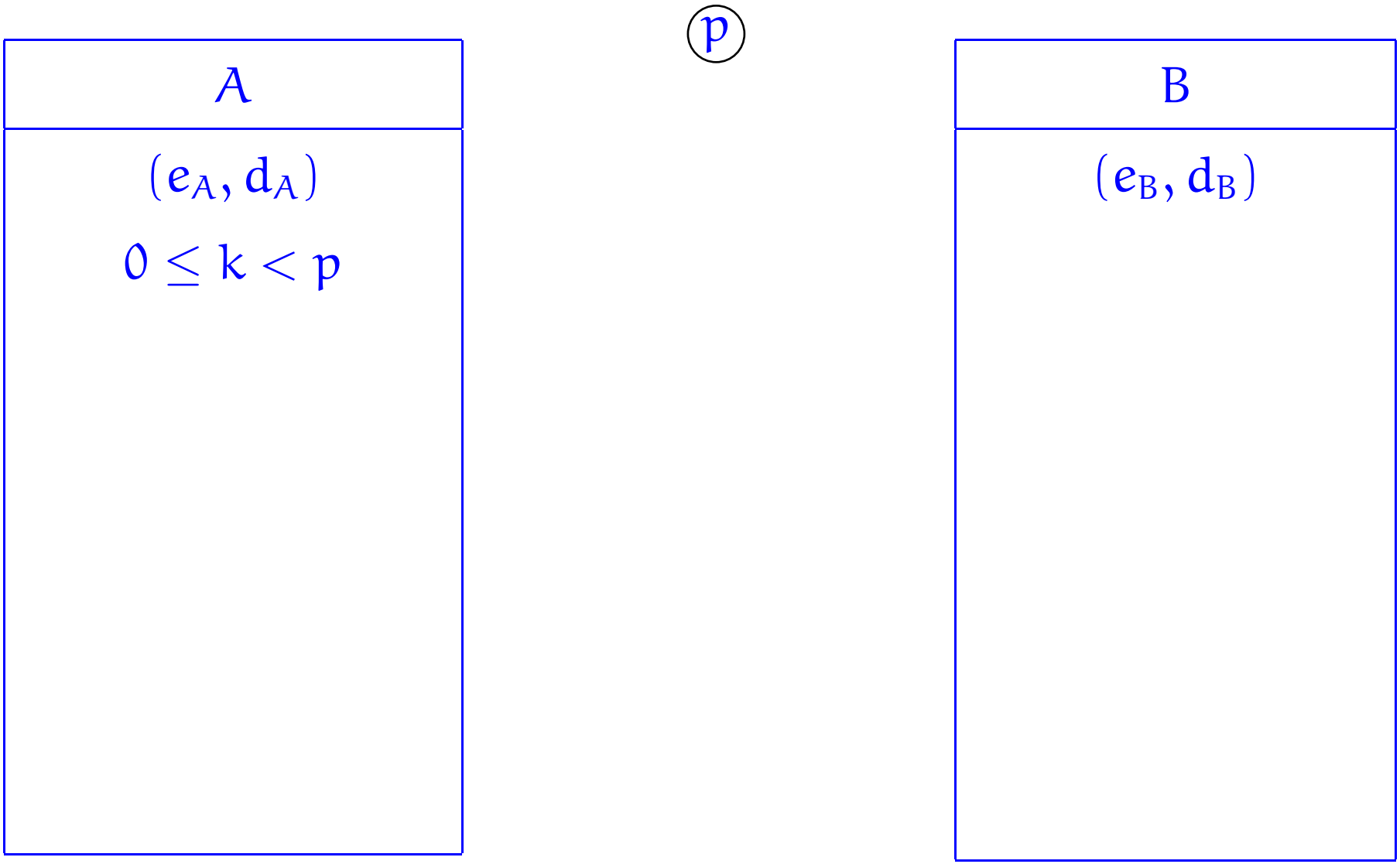
FLT

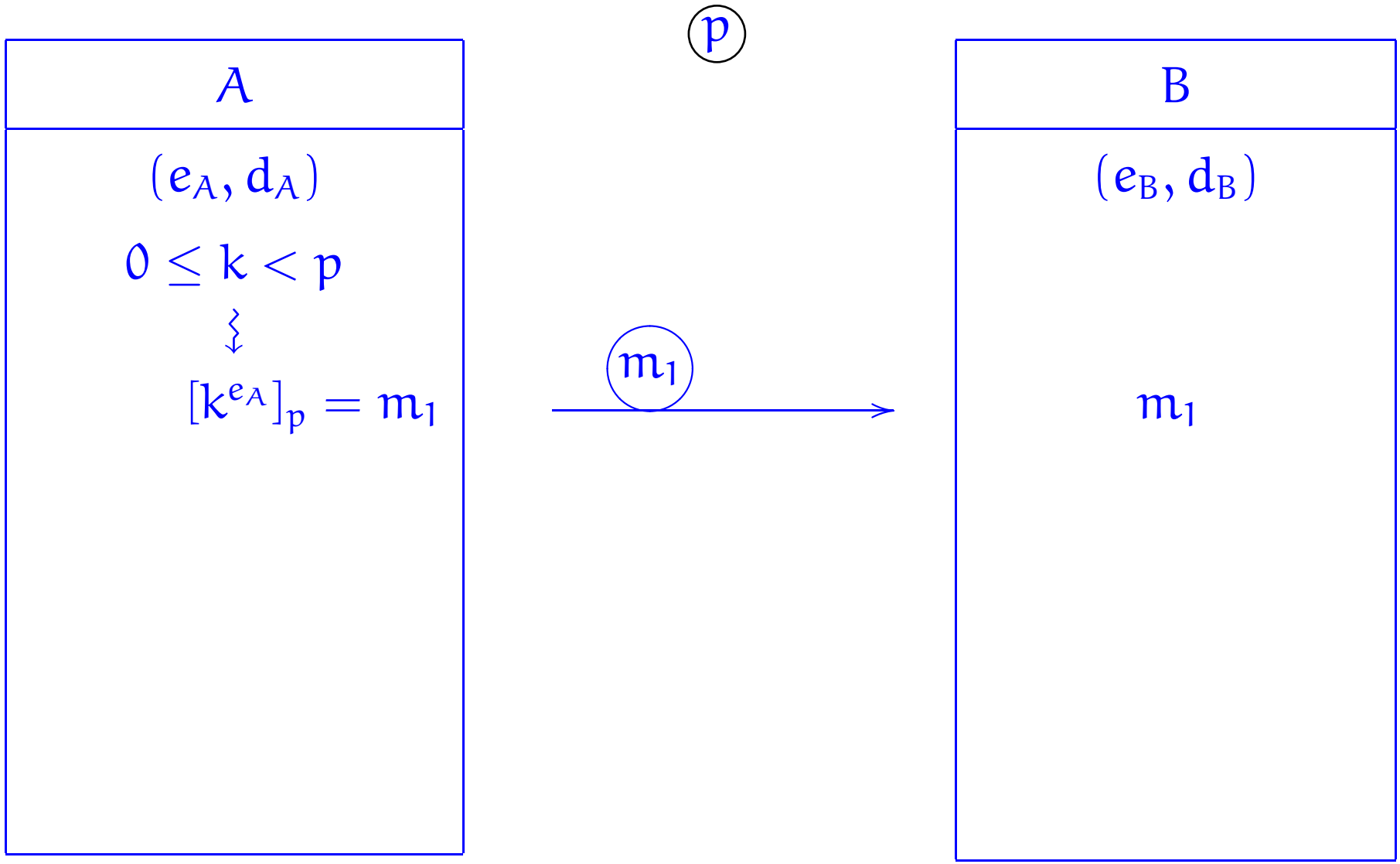
① $i^p \equiv i \pmod p$

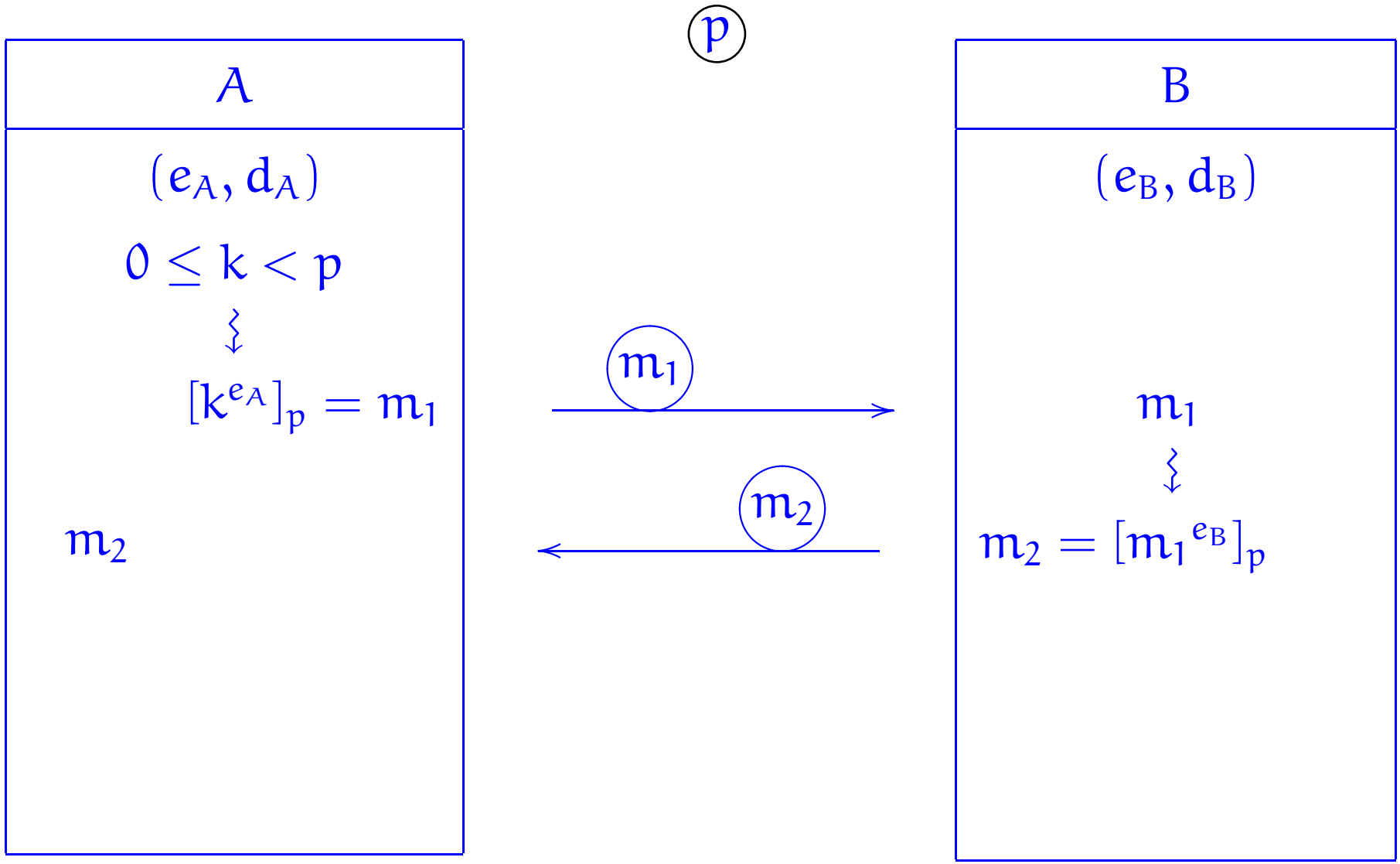
② $i^{p-1} \equiv 1 \pmod p$

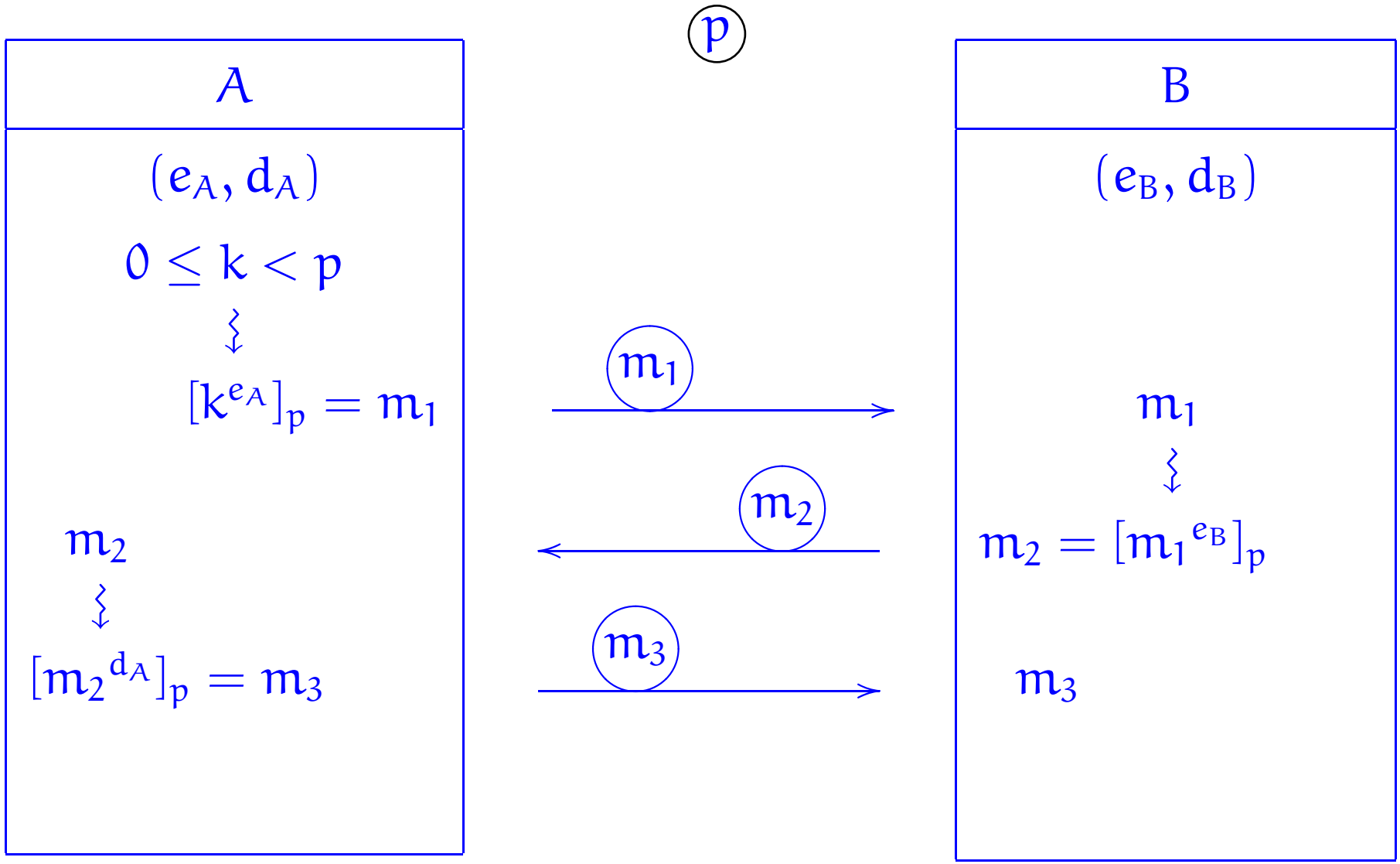
$\Big\}$ $i \not\equiv 0 \pmod p$

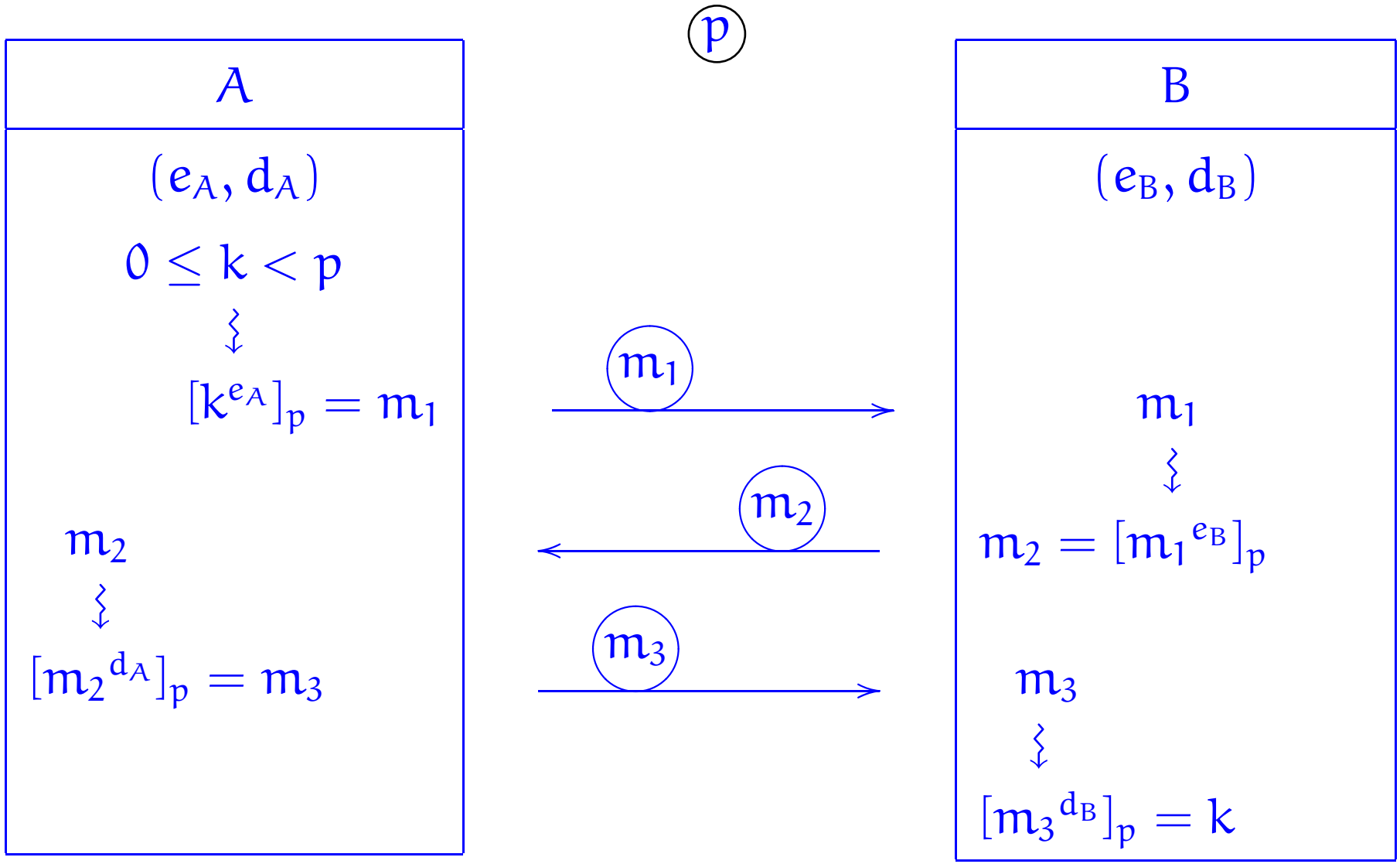

A
B


p
A
(e_A, d_A)
$0 \leq k < p$
B
(e_B, d_B)


p
A
(e_A, d_A)
$0 \leq k < p$
$[k^{e_A}]_p = m_1$
m_1
B
(e_B, d_B)
m_1


p
A
(e_A, d_A)
$0 \leq k < p$
$[k^{e_A}]_p = m_1$
m_2
m_1
m_2
B
(e_B, d_B)
m_1
$m_2 = [m_1{}^{e_B}]_p$


p
A
B
(e_A, d_A)
$0 \leq k < p$
$[k^{e_A}]_p = m_1$
m_2
$[m_2{}^{d_A}]_p = m_3$
m_1
m_2
m_3
(e_B, d_B)
m_1
$m_2 = [m_1{}^{e_B}]_p$
m_3



$$\left[\left[\left[k^{e_A}\right]_p{}^{e_B}\right]_p{}^{d_A}\right]_p = \left[\left[\left[k^{e_A}\right]_p{}^{d_A}\right]_p{}^{e_B}\right]_p = \left[k^{e_B}\right]_p$$

Natural Numbers and mathematical induction

We have mentioned in passing that the natural numbers are generated from zero by succesive increments. This is in fact the defining property of the set of natural numbers, and endows it with a very important and powerful reasoning principle, that of *Mathematical Induction*, for establishing universal properties of natural numbers.

Principle of Induction

Let $P(m)$ be a statement for m ranging over the set of natural numbers $\mathbb{N}$.

If

BASE CASE:

- the statement $P(0)$ holds, and

INDUCTIVE STEP:

- the statement

$$\forall n \in \mathbb{N}.\ \big(\ P(n) \implies P(n+1)\ \big)$$

  also holds

then

- the statement

$$\forall m \in \mathbb{N}.\, P(m)$$

  holds.

Binomial Theorem

Theorem 29 *For all* $n \in \mathbb{N}$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k \quad .$$

PROOF: A non-trivial exercise.

Thm: $\forall n \in \mathbb{N}.\ Even(n) \vee Odd(n)$

where $Even(n) \stackrel{def}{=} (\exists i \in \mathbb{N}.\ n = 2i)$

and $Odd(n) \stackrel{def}{=} (\exists j \in \mathbb{N}.\ n = 2j+1)$.

PROOF: We proceed by induction.

Base case: RTP: $Even(0) \vee Odd(0)$

But $0 = 2 \cdot 0$ Hence $Even(0)$ holds and we are done.

Inductive step: Let $n \in \mathbb{N}$, assume

$Even(n) \vee Odd(n)$ (*)

RTP: $Even(n+1) \vee Odd(n+1)$ (**)

By (*):

Assume: $Even(n)$

RTP: (**)

$\Rightarrow \exists i \in \mathbb{N}.\ n = 2i$

$\Rightarrow \exists i \in \mathbb{N}.\ n+1 = 2i+1$

$\Rightarrow Odd(n+1)$

$\Rightarrow$ (**) ☒

Assume: $Odd(n)$

RTP (**)

$\Rightarrow \exists j \in \mathbb{N}.\ n = 2j+1$

$\Rightarrow \exists j' \in \mathbb{N}.\ n+1 = 2j'$

$\Rightarrow Even(n+1)$

$\Rightarrow$ (**) ☒

Principle of Induction

from basis ℓ

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.
If

- $P(\ell)$ holds, and
- $\forall\, n \geq \ell$ in $\mathbb{N}$. $\big(\, P(n) \implies P(n+1) \,\big)$ also holds

then

- $\forall\, m \geq \ell$ in $\mathbb{N}$. $P(m)$ holds.

Principle of Strong Induction

from basis ℓ and Induction Hypothesis $P(m)$.

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.

If both

- $P(\ell)$ and
- $\forall\, n \geq \ell$ in $\mathbb{N}.\ \Big(\big(\forall\, k \in [\ell..n].\, P(k) \big) \implies P(n+1) \Big)$

hold, then

- $\forall\, m \geq \ell$ in $\mathbb{N}.\, P(m)$ holds.