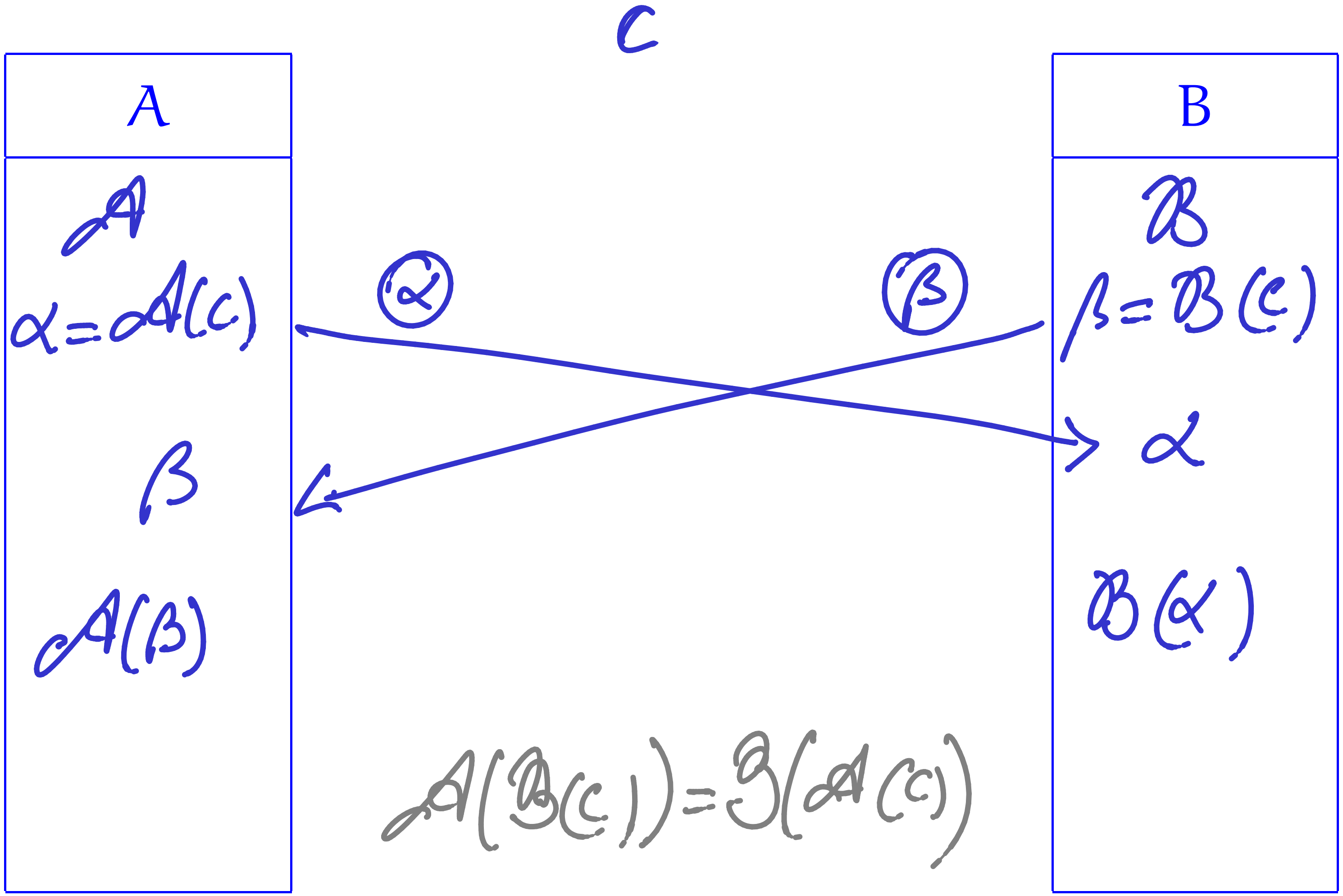
Application to Public-Key Cryptography

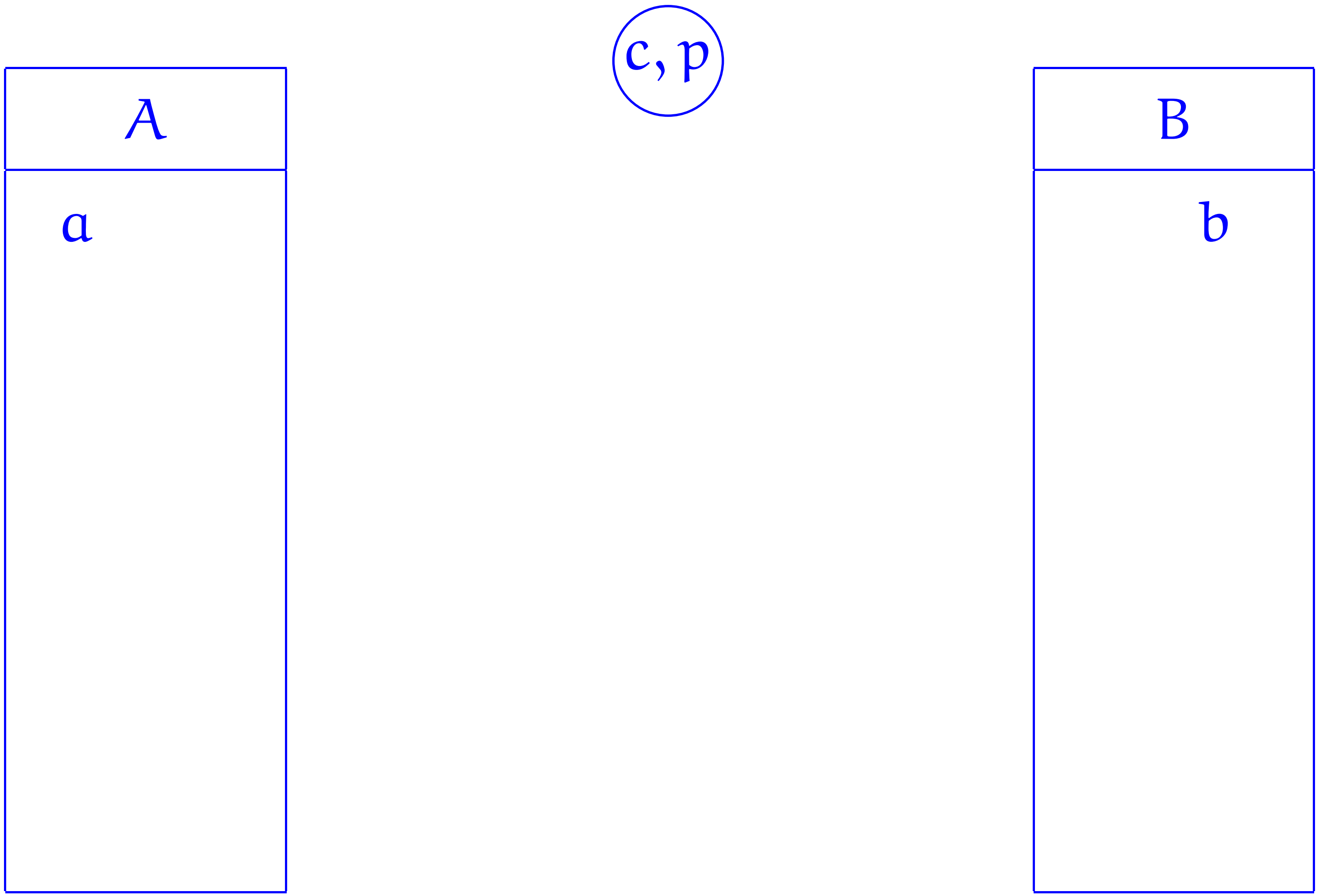
Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

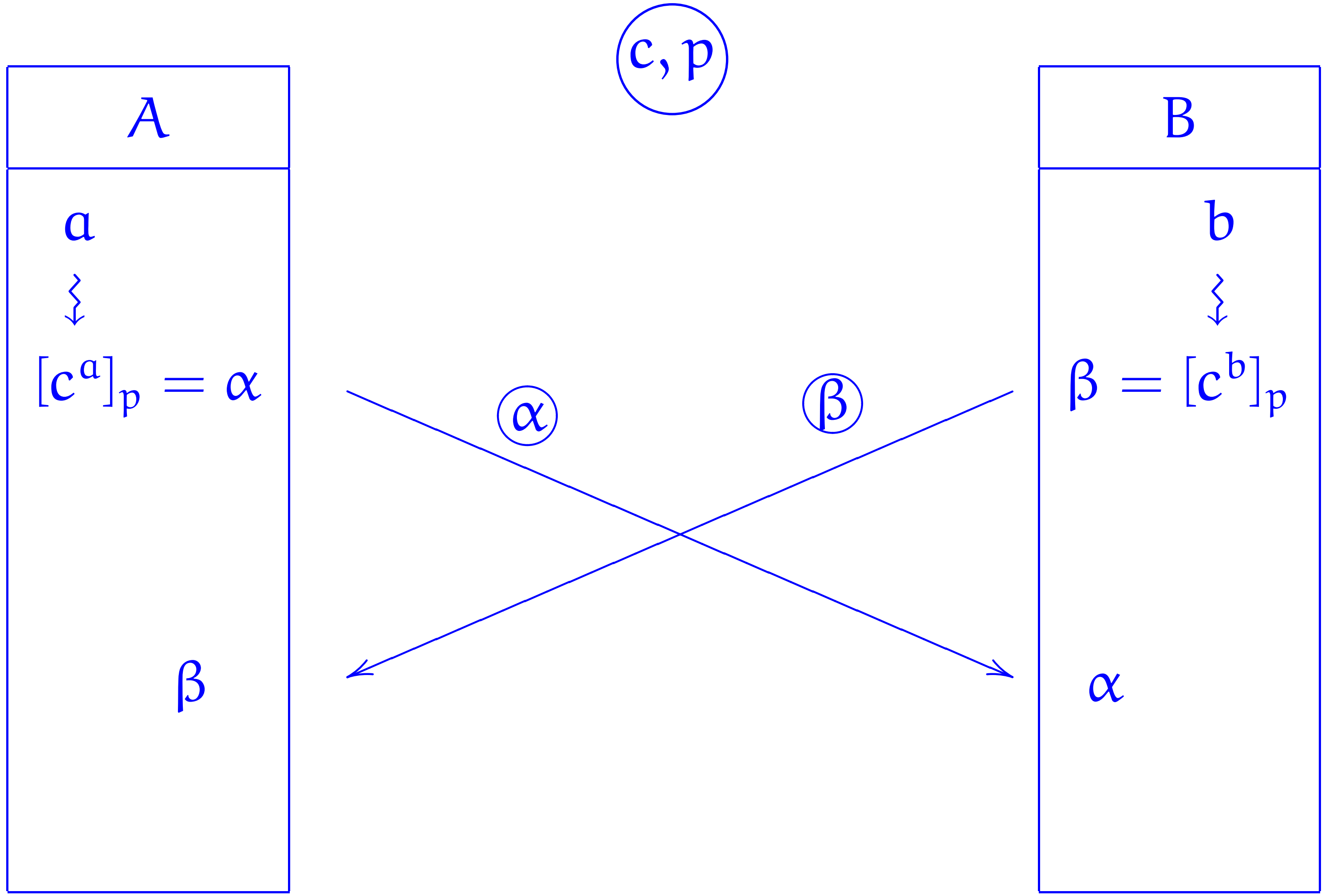
Shared secret key

c, p

A	B
a	b
$\rightsquigarrow$	$\rightsquigarrow$
$[c^a]_p = \alpha$	$\beta = [c^b]_p$

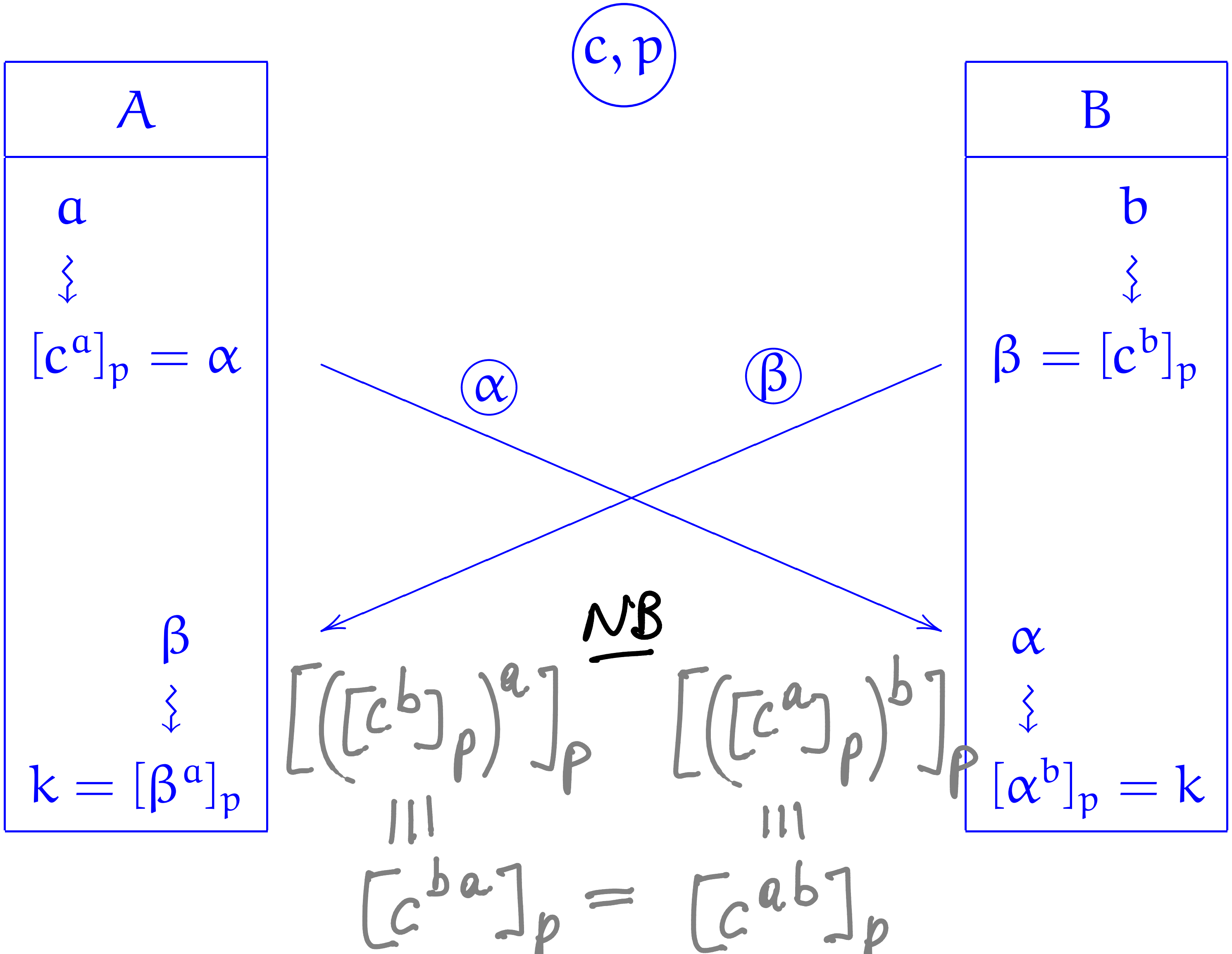
Diffie-Hellman cryptographic method

Shared secret key

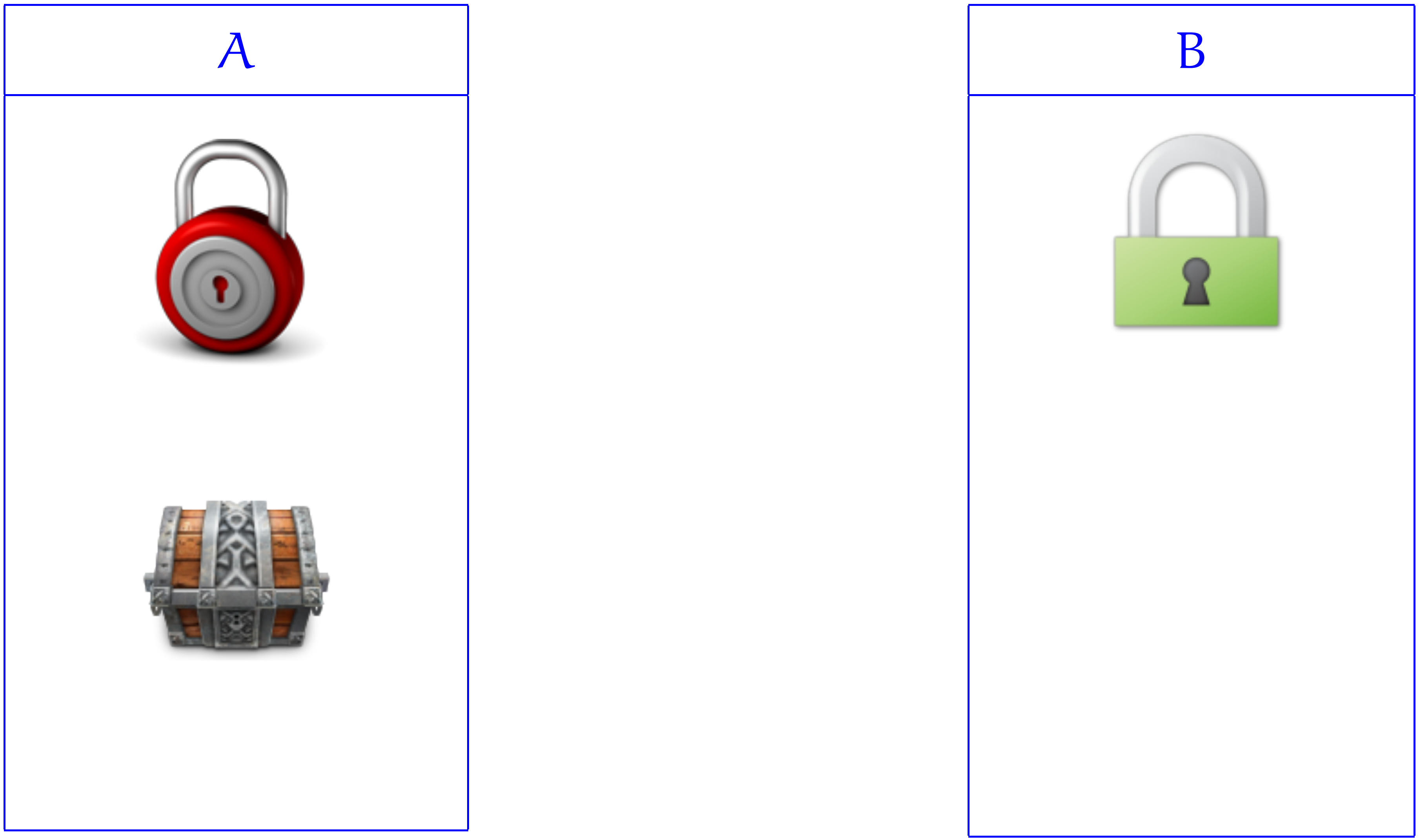


Diffie-Hellman cryptographic method

Shared secret key



Key exchange

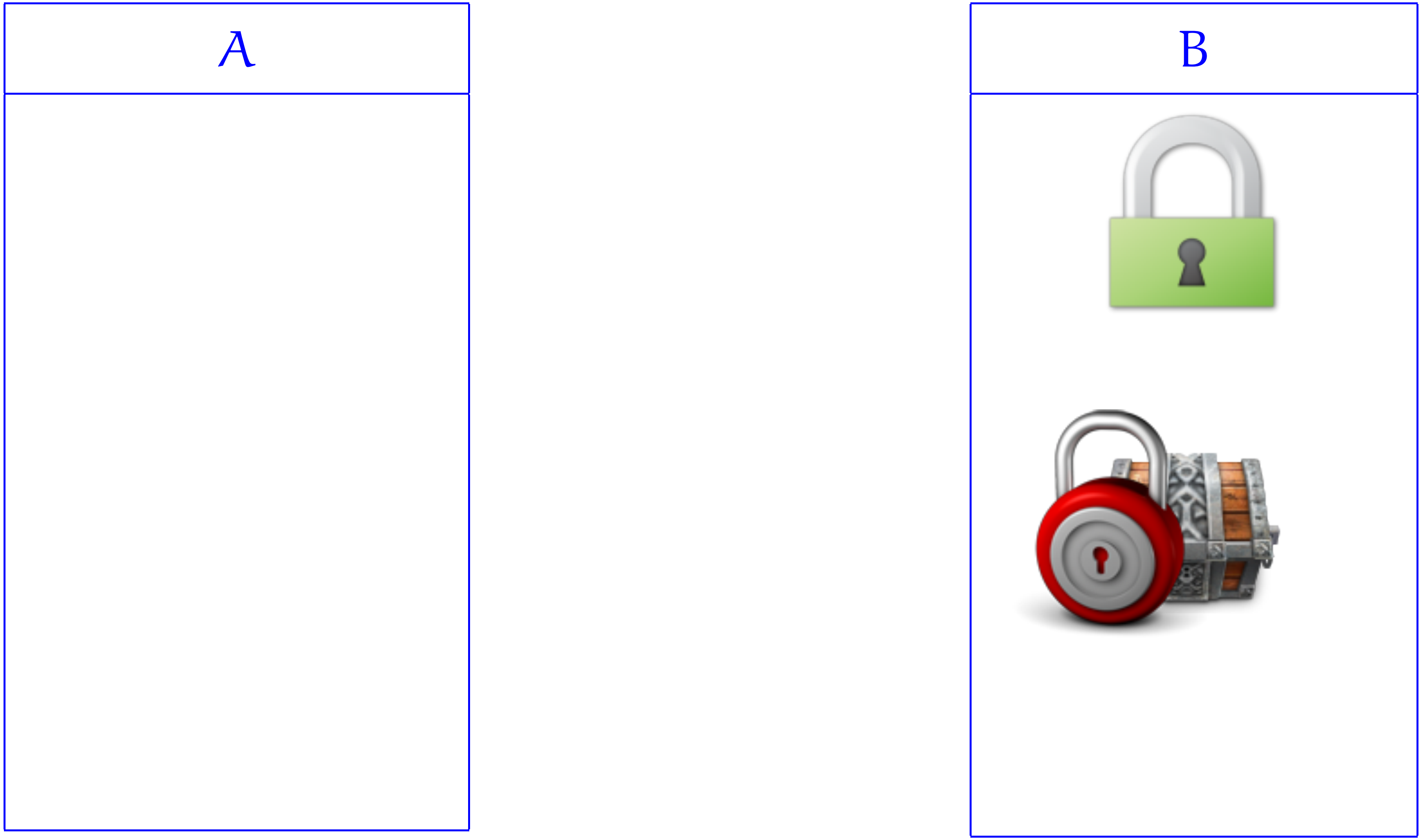


Key exchange

A

B

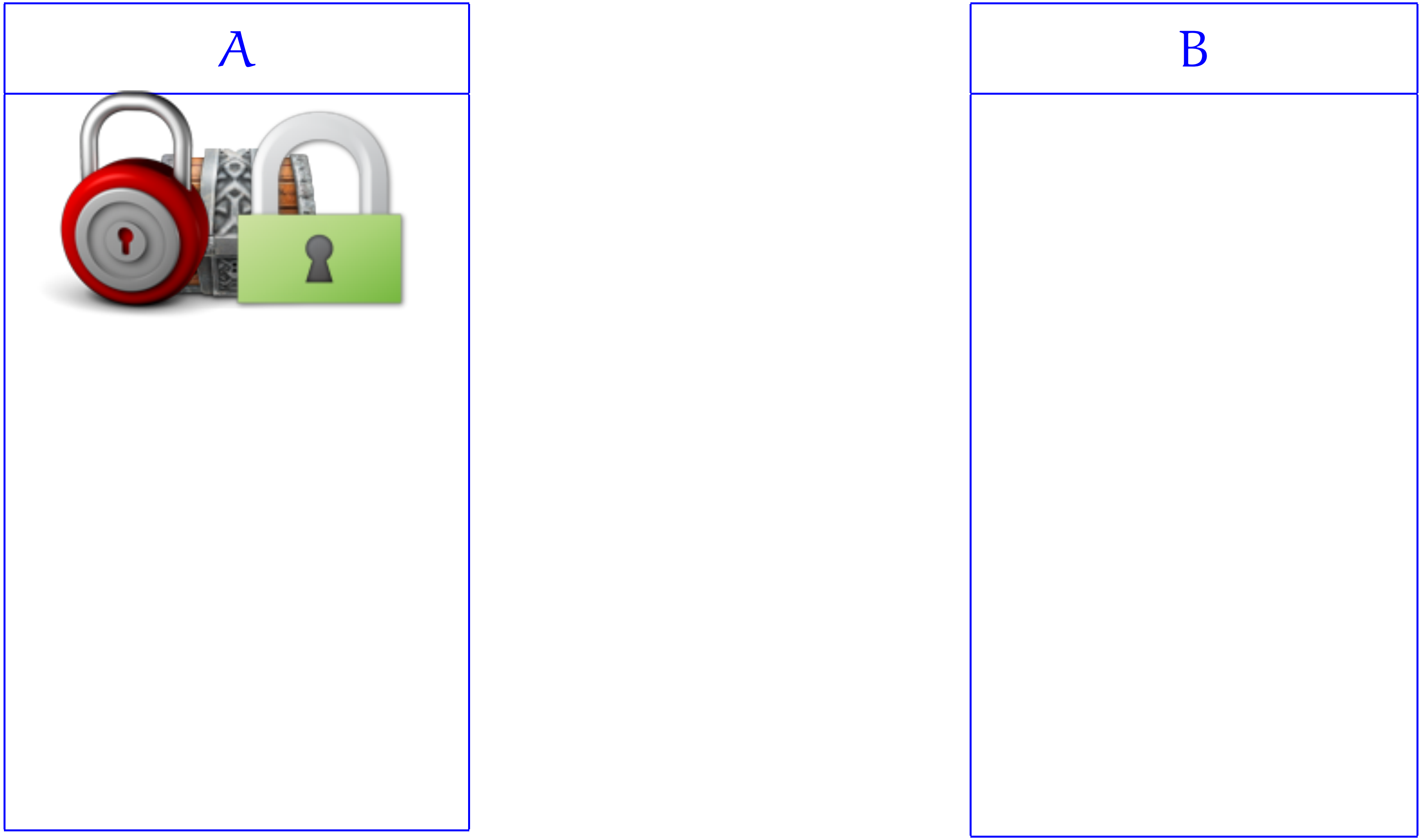
Key exchange



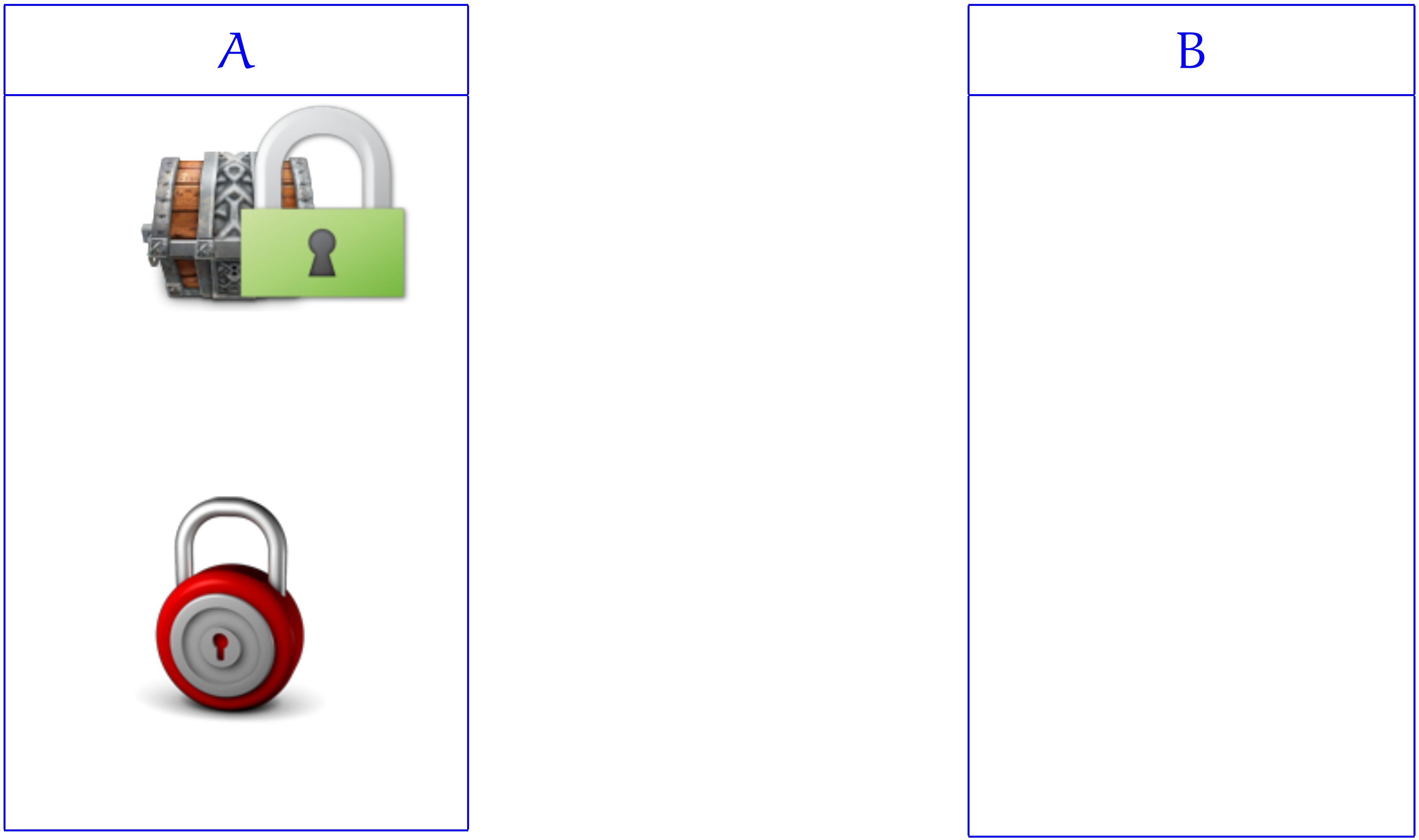
Key exchange

A	B
	

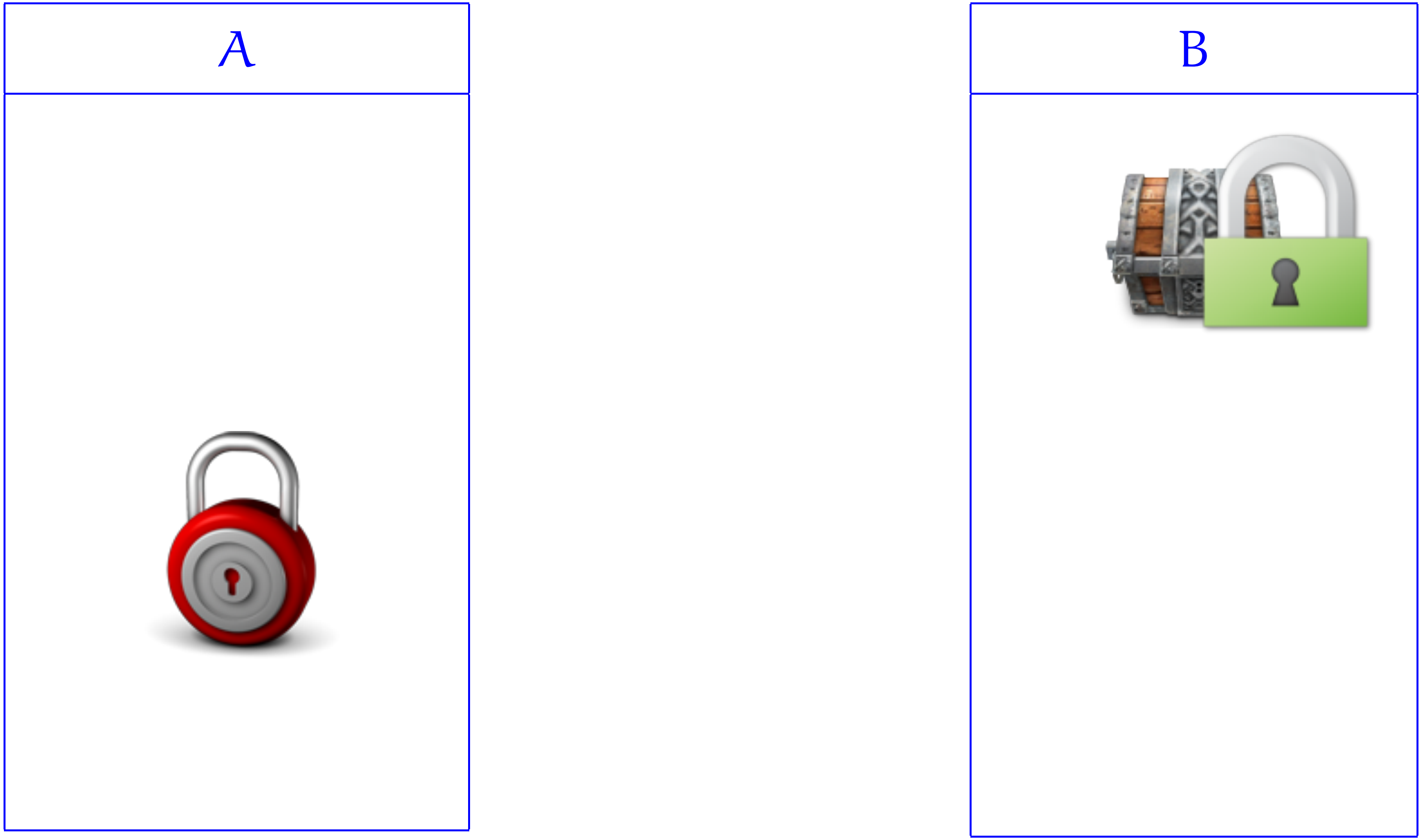
Key exchange



Key exchange



Key exchange



Key exchange

Mathematical modelling:

- Lock/encrypt and unlock/decrypt by means of modular exponentiation

$$[k^e]_p \qquad [\ell^d]_p$$

- Locking-unlocking/encrypting-decrypting have no effect.

FLT: $\forall$ nat. numbers c, $\forall$ int k:

$$k^{1+c(p-1)} \equiv k \pmod p$$

- Consider d, e, p such that $ed = 1 + c(p-1)$; equivalently, $de \equiv 1 \pmod p$.

Key exchange

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

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

Then, for all integers k,

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

PROOF:

PROOF: Let p be a prime and e be a positive integer such that $\underline{gcd}(p-1, e) = 1$; so that, writing $l_1 =^{def} \underline{lc}_1(p-1, e)$ and $l_2 =^{def} \underline{lc}_2(p-1, e)$ we have

$$l_1 (p-1) + l_2 e = 1 \qquad (l_1, l_2 \text{ integers})$$

Let $d =^{def} [l_2]_{p-1}$ in $\mathbb{Z}_{p-1}$; so that

$$d = l_2 + m(p-1) \qquad (0 < d < p-1, \; m \text{ integer})$$

(btw, d is the reciprocal of $[e]_{p-1}$ in $\mathbb{Z}_{p-1}$).

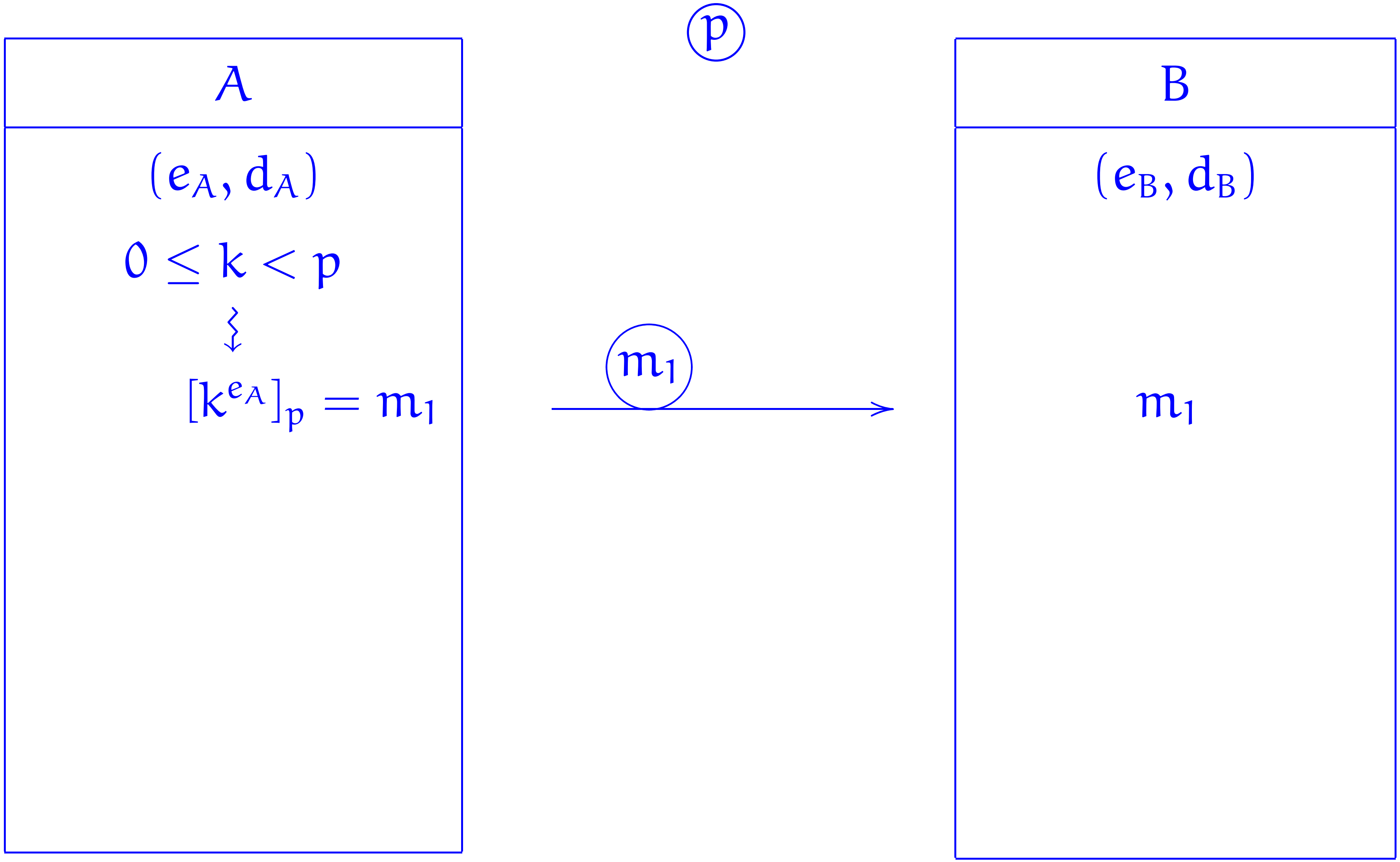
Then,
$$k^{ed} = k^{1 + \underbrace{(me - l_1)}_{\text{a natural number}} \cdot (p-1)} \underset{\text{by FLT}}{\equiv} k \pmod p$$

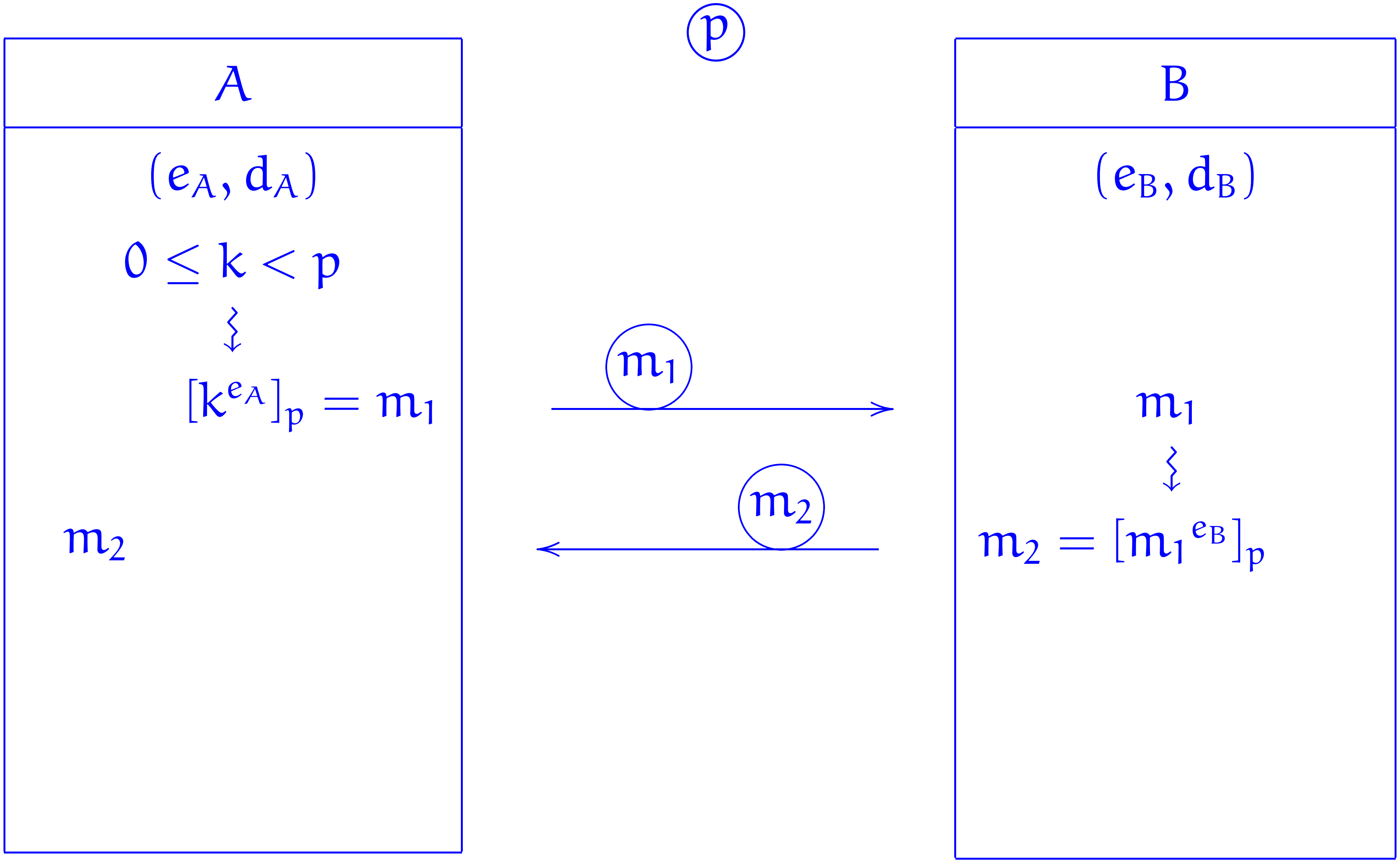
$\boxtimes$

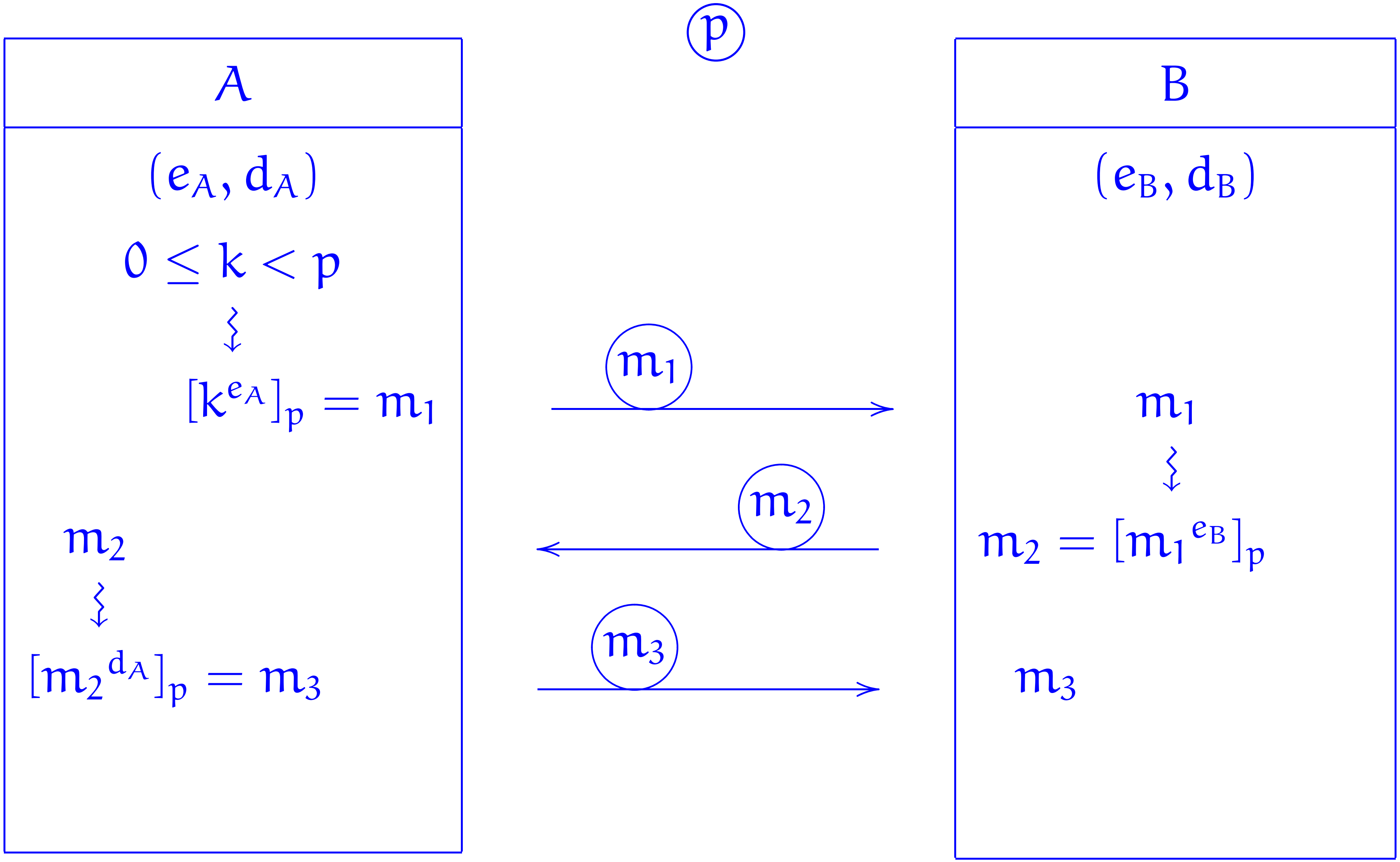
Key exchange

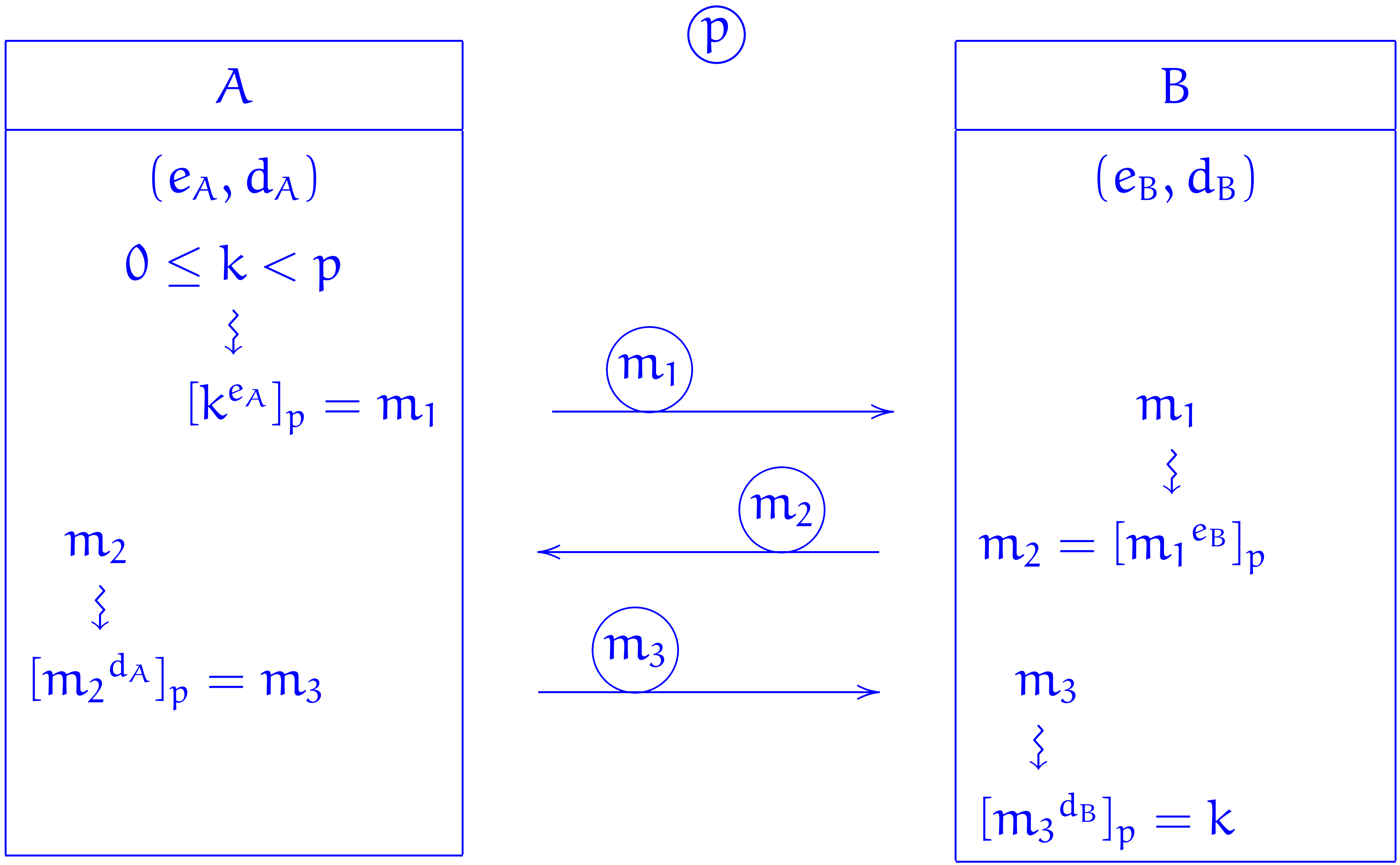
$\textcircled{p}$

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


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


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


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



p
A
(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
B
(e_B, d_B)
m_1
$m_2 = [{m_1}^{e_B}]_p$
m_3
$[{m_3}^{d_B}]_p = k$

Encryption/Decrytion in RSA

Lemma: Let p, q be distinct primes and d, e be positive integers such that $e \cdot d \equiv 1 \pmod{(p-1)\cdot(q-1)}$. Then, for all integers k,

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

PROOF: Let p, q be distinct primes and let e, d be positive integers such that

$$i \cdot (p-1)(q-1) + e \cdot d = 1$$

for an integer i.

Show that for k integer

① $(k^e)^d \equiv k \pmod{p}$

and ② $(k^e)^d \equiv k \pmod{q}$

Argue that

③ $(k^e)^d \equiv k \pmod{p \cdot q}$

☒