Extended Euclid's Algorithm

	$\gcd(34, 13)$	$8 =$	34	$-2\cdot$	13
$=$	$\gcd(13, 8)$	$5 =$	13	$-1\cdot$	8
$=$	$\gcd(8, 5)$	$3 =$	8	$-1\cdot$	5
$=$	$\gcd(5, 3)$	$2 =$	5	$-1\cdot$	3
$=$	$\gcd(3, 2)$	$1 =$	3	$-1\cdot$	2

Extended Euclid's Algorithm

$$
\begin{array}{rl||rcccc}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & = & -1\cdot 34 + 3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

Extended Euclid's Algorithm

$$
\begin{array}{rl||rcccc}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & = & \overbrace{(34-2\cdot 13)} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)} \\
 & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

Extended Euclid's Algorithm

$$
\begin{array}{rl||rcccc}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & = & \overbrace{(34-2\cdot 13)} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)} \\
 & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & = & \overbrace{-1\cdot 34+3\cdot 13} & -1\cdot & \overbrace{(2\cdot 34+(-5)\cdot 13)} \\
 & & = & -3\cdot 34+8\cdot 13 & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

Extended Euclid's Algorithm

$\gcd(m,n) = l_1 \cdot m + l_2 \cdot n$ for integers l_1 and l_2

$$
\begin{array}{rl|l}
 & \gcd(34,13) & 8 = 34 - 2 \cdot 13 \\
= & \gcd(13,8) & 5 = 13 - 1 \cdot 8 \\
 & & \quad = 13 - 1 \cdot \overbrace{(34 - 2 \cdot 13)}^{8} \\
 & & \quad = -1 \cdot 34 + 3 \cdot 13 \\
= & \gcd(8,5) & 3 = 8 - 1 \cdot 5 \\
 & & \quad = \overbrace{(34 - 2 \cdot 13)}^{8} - 1 \cdot \overbrace{(-1 \cdot 34 + 3 \cdot 13)}^{5} \\
 & & \quad = 2 \cdot 34 + (-5) \cdot 13 \\
= & \gcd(5,3) & 2 = 5 - 1 \cdot 3 \\
 & & \quad = \overbrace{-1 \cdot 34 + 3 \cdot 13}^{5} - 1 \cdot \overbrace{(2 \cdot 34 + (-5) \cdot 13)}^{3} \\
 & & \quad = -3 \cdot 34 + 8 \cdot 13 \\
= & \gcd(3,2) & 1 = 3 - 1 \cdot 2 \\
 & & \quad = \overbrace{(2 \cdot 34 + (-5) \cdot 13)}^{3} - 1 \cdot \overbrace{(-3 \cdot 34 + 8 \cdot 13)}^{2}) \\
 & & \quad = 5 \cdot 34 + (-13) \cdot 13
\end{array}
$$

ex. $1 = l_1 \cdot 34 + l_2 \cdot 13$ where $l_1 = 5$ and $l_2 = -13$

or integer linear combination

Linear combinations

Definition 68 *An integer* r *is said to be a* linear combination *of a pair of integers* m *and* n *whenever*

> *there exist a pair of integers* s *and* t*, referred to as the* coefficients *of the linear combination, such that*
>
> $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \; ;$$
>
> NB Could take k such that $0 \leq t - km < m$
>
> *that is*
>
> $$s \cdot m + t \cdot n = r \; .$$

$\Rightarrow \quad (s + kn) \cdot m + (t - km) \cdot n = r \quad \forall\, k \in \mathbb{Z}$

Theorem 69 *For all positive integers* m *and* n*,*

1. $\mathrm{gcd}(m, n)$ *is a linear combination of* m *and* n*, and*
2. *a pair* $\mathrm{lc}_1(m, n)$, $\mathrm{lc}_2(m, n)$ *of integer coefficients for it, i.e. such that*

$$\begin{bmatrix} \mathrm{lc}_1(m, n) & \mathrm{lc}_2(m, n) \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = \mathrm{gcd}(m, n) \quad ,$$

can be efficiently computed.

m is a l.c. of m and n with coeff. 1 and 0

Proposition 70 *For all integers* m *and* n,

1. $\begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \;\wedge\; \begin{bmatrix} 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

2. *for all integers* s_1, t_1, r_1 *and* s_2, t_2, r_2,

$$\begin{bmatrix} s_1 & t_1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 \;\wedge\; \begin{bmatrix} s_2 & t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_2$$

   implies

$$\begin{bmatrix} s_1 + s_2 & t_1 + t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \;;$$

3. *for all integers* k *and* s, t, r,

$$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \;\textit{implies}\; \begin{bmatrix} k \cdot s & k \cdot t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = k \cdot r \;.$$

Say r_1 has coeff s_1 and t_1

and r_2 has coeff s_2 and t_2

[?] What are the coeff of $r = r_1 - q \cdot r_2$?

$= r_1 + (-q) \cdot r_2$

We know $(-q) \cdot r_2$ has coeff $(-q) \cdot s_2$ and $(-q) \cdot t_2$

So $r_1 + (-q) \cdot r_2$ has coeff $s_1 + (-q) \cdot s_2$ and $t_1 + (-q) \cdot t_2$.

Coefficients

gcd

```
fun  gcd( m , n )
= let
    fun  gcditer(          r1   ,   c as          r2   )
    = let
        val (q,r) = divalg(r1,r2)    (* r = r1-q*r2 *)
      in
        if r = 0
        then  c
        else  gcditer(  c ,                       r   )
      end
  in
    gcditer(         m   ,        n   )
  end
```

egcd

```
fun egcd( m , n )
= let
    fun egcditer( ((s1,t1),r1) , lc as ((s2,t2),r2) )
    = let
        val (q,r) = divalg(r1,r2)    (* r = r1-q*r2 *)
      in
        if r = 0
        then lc
        else egcditer( lc , ((s1-q*s2,t1-q*t2),r) )
      end
  in
    egcditer( ((1,0),m) , ((0,1),n) )
  end
```

```
fun gcd( m , n ) = #2( egcd( m , n ) )

fun lc1( m , n ) = #1( #1( egcd( m , n ) ) )

fun lc2( m , n ) = #2( #1( egcd( m , n ) ) )
```

because: $gcd(m,n) = l_1 \cdot m + l_2 \cdot n$

Multiplicative inverses in modular arithmetic

Corollary 74 *For all positive integers* m *and* n*,*

1. $n \cdot \mathrm{lc}_2(m,n) \equiv \gcd(m,n) \pmod{m}$*, and*

2. *whenever* $\gcd(m,n) = 1$*,*

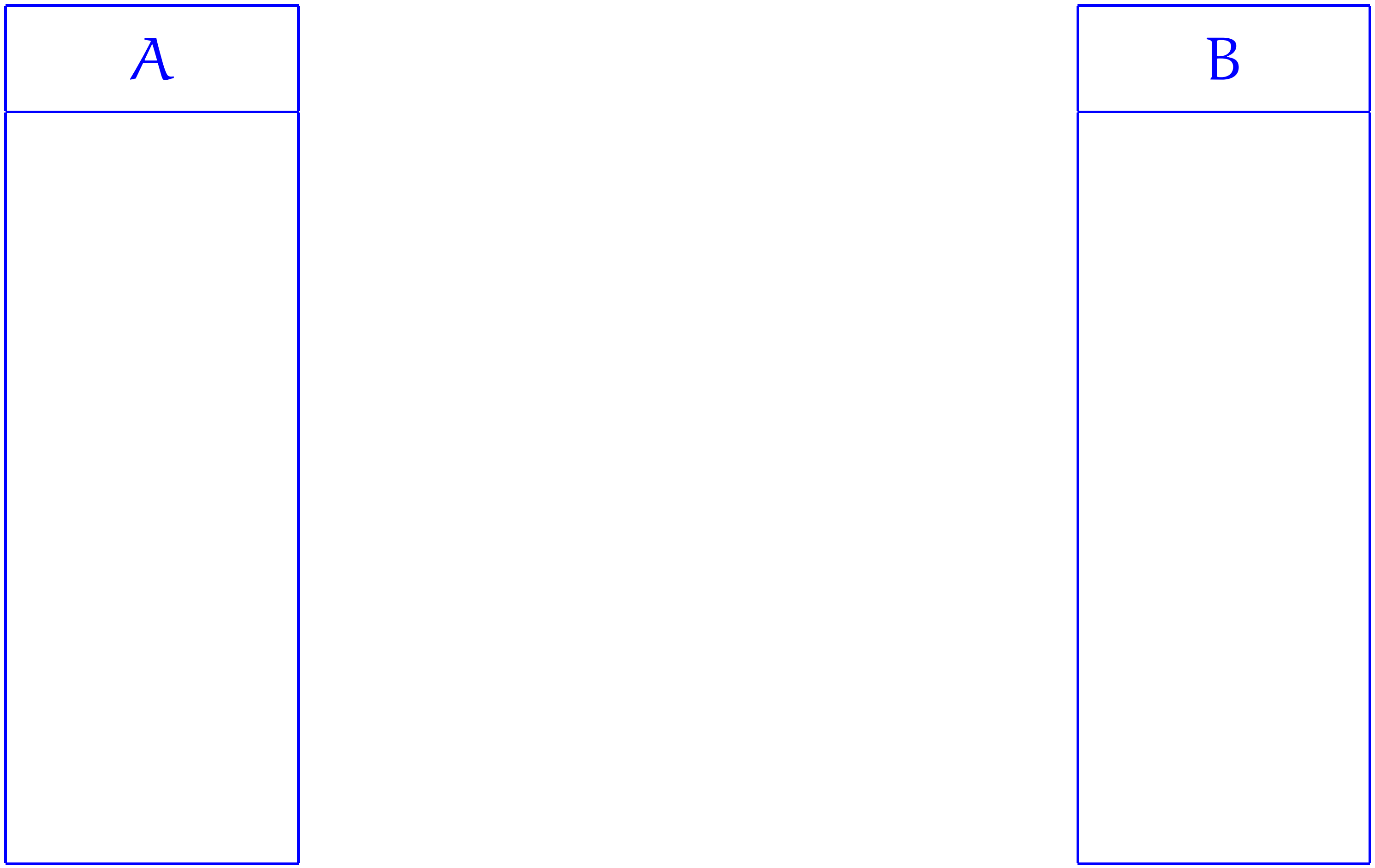
   $\mathbb{Z}_m \ni \left[\mathrm{lc}_2(m,n)\right]_m$ *is the multiplicative inverse of* $[n]_m$ *in* $\mathbb{Z}_m$.

   $\equiv$ $lc_2(m,n) \pmod{m}$

$n \cdot l_2 \equiv 1 \pmod{m}$

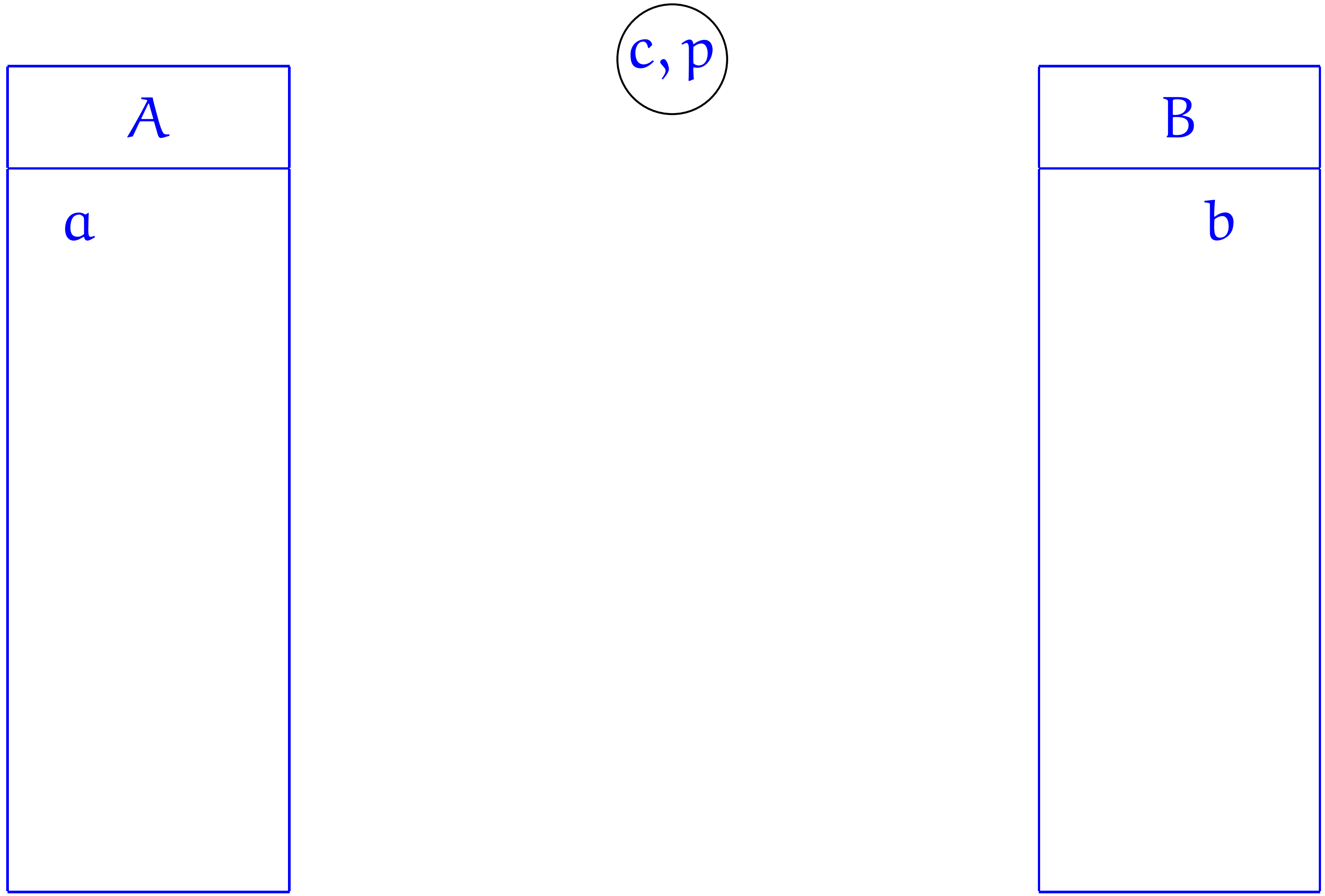
Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

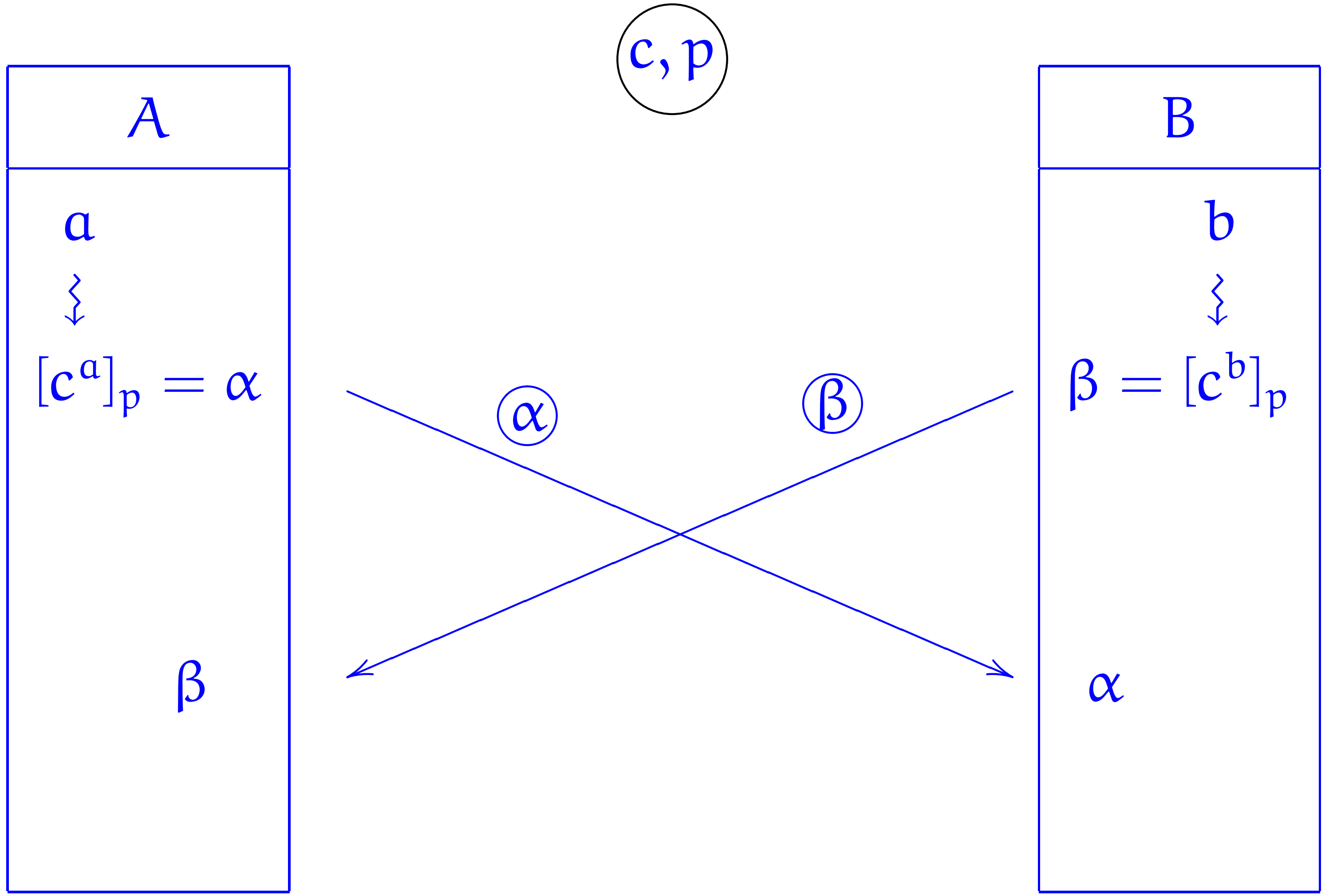
Shared secret key

c, p

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

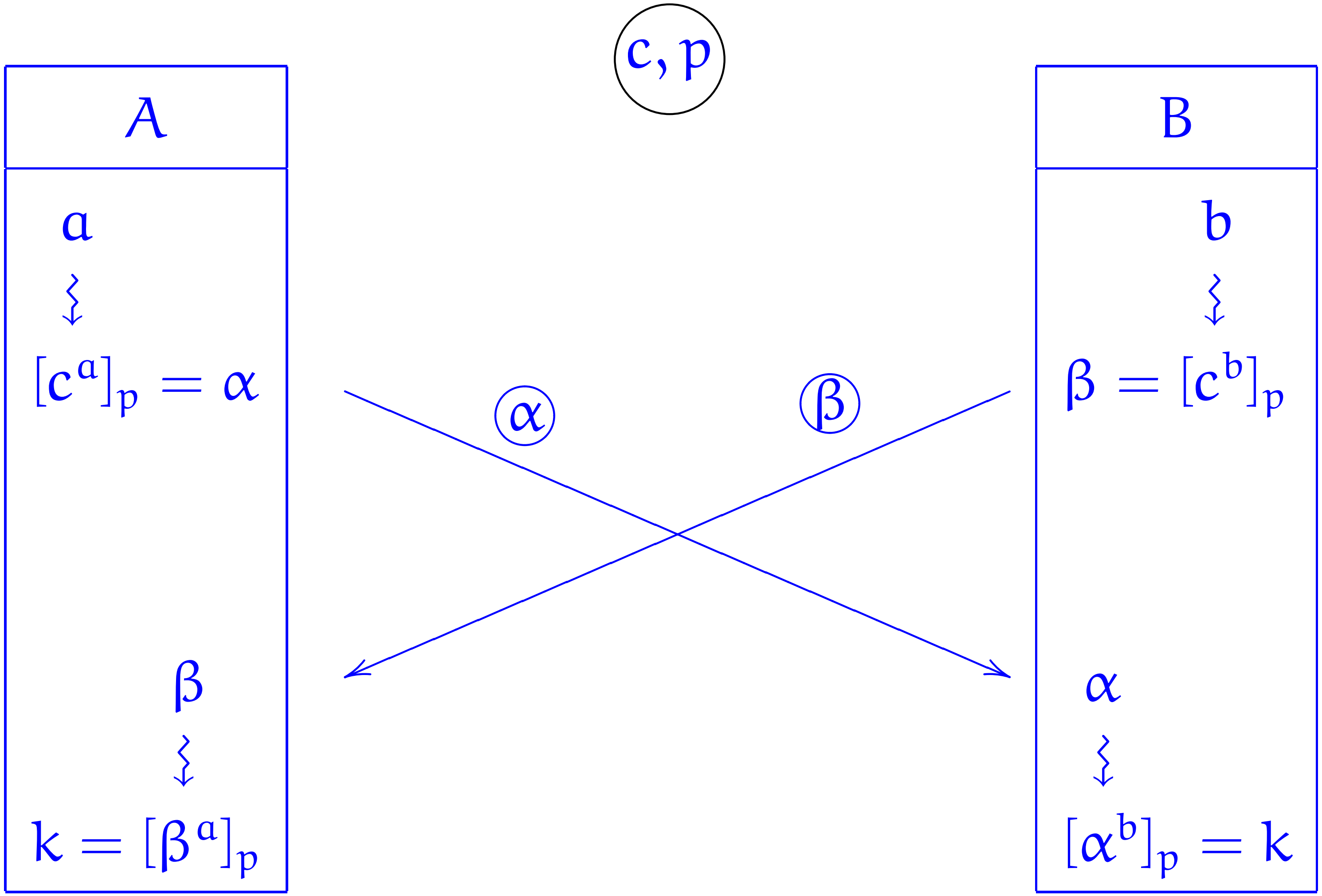
Diffie-Hellman cryptographic method

Shared secret key

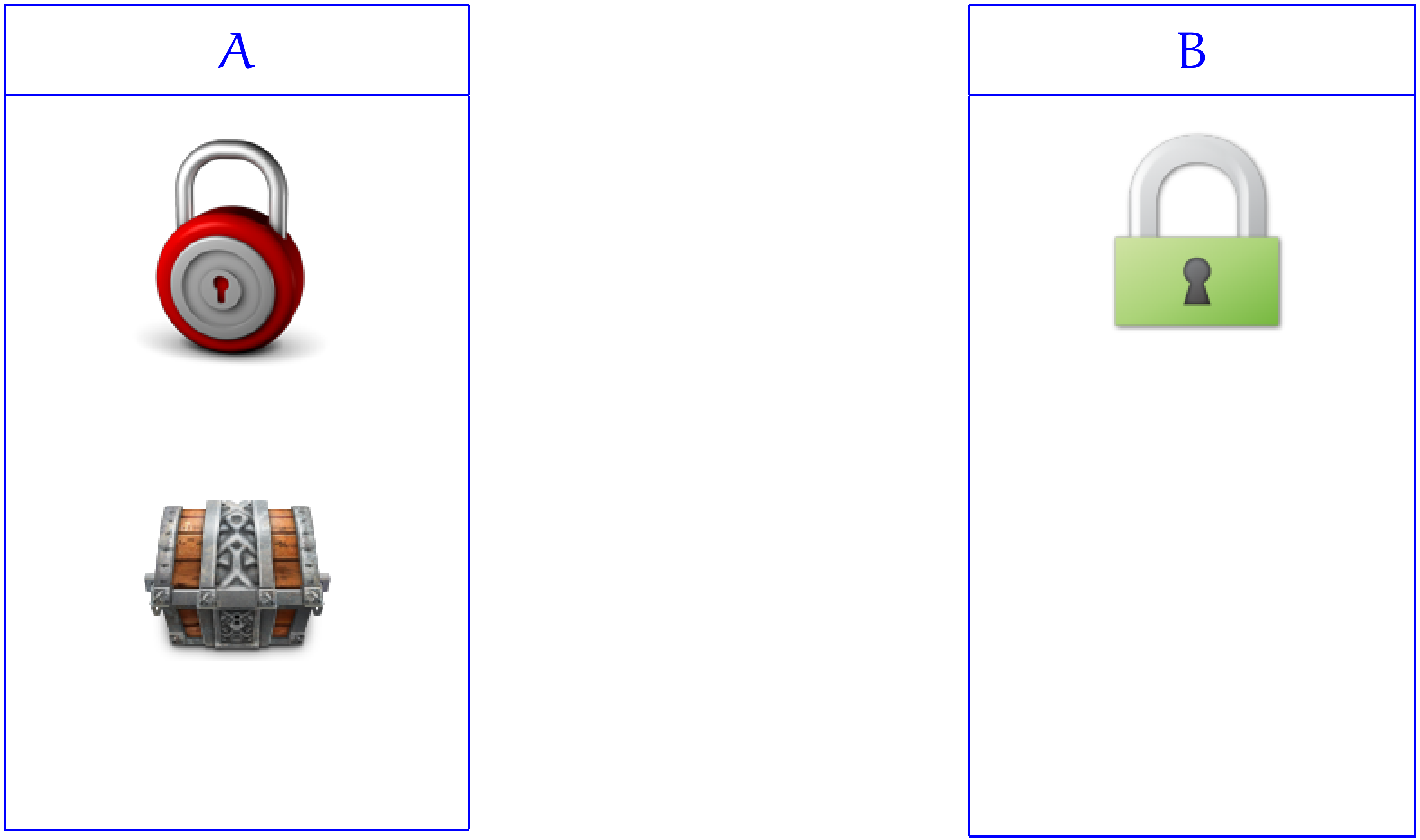


Diffie-Hellman cryptographic method

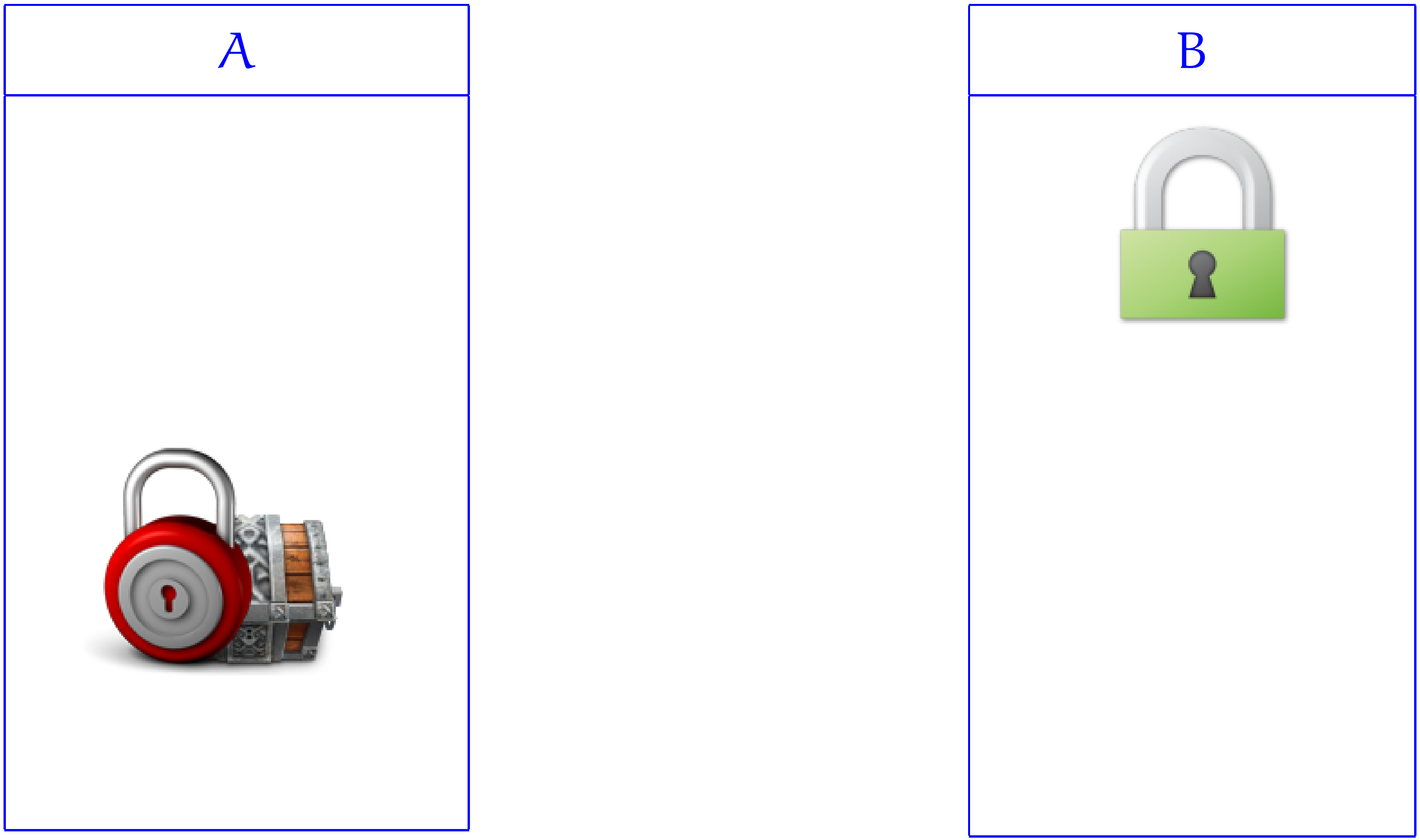
Shared secret key



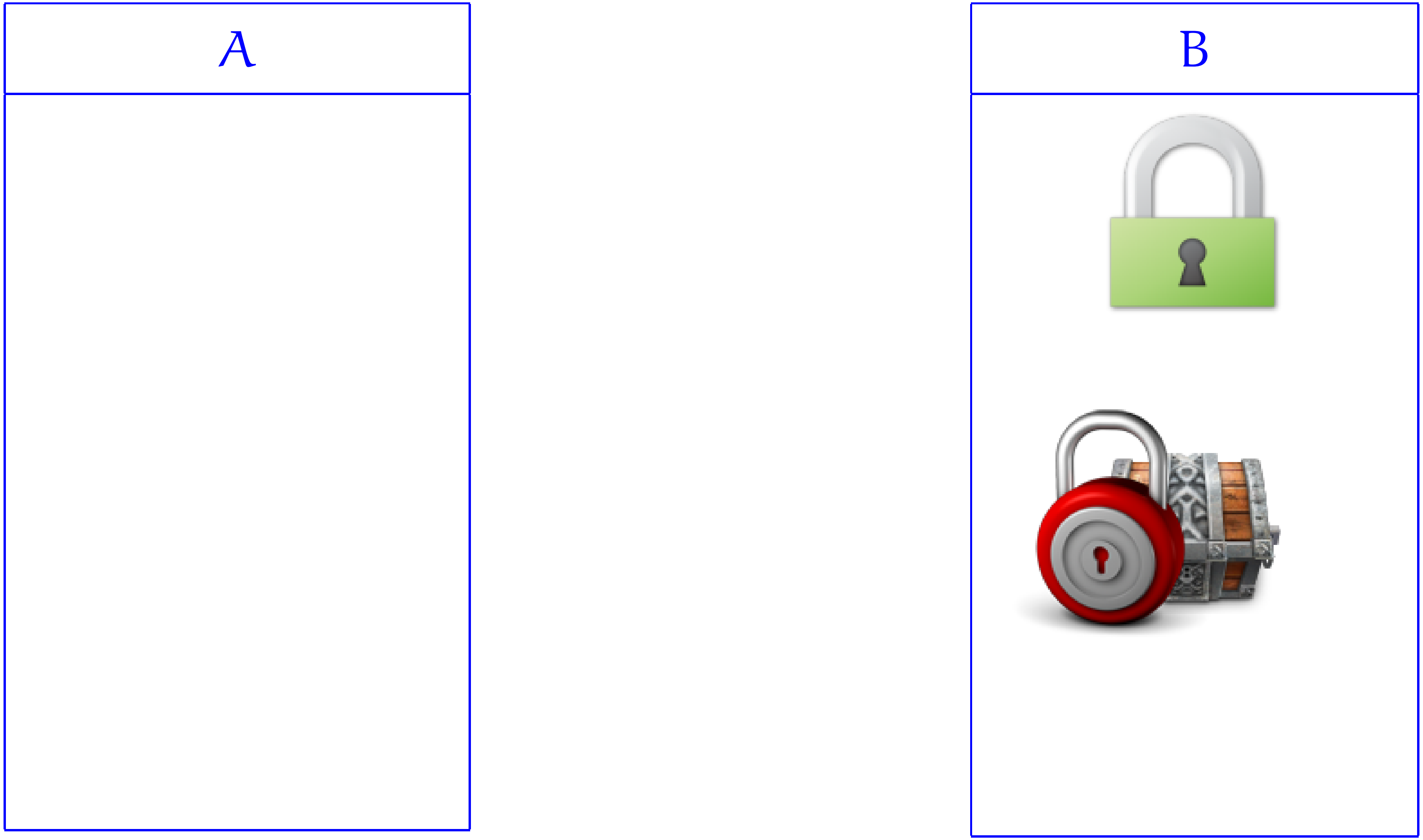
Key exchange



Key exchange



Key exchange



Key exchange

A

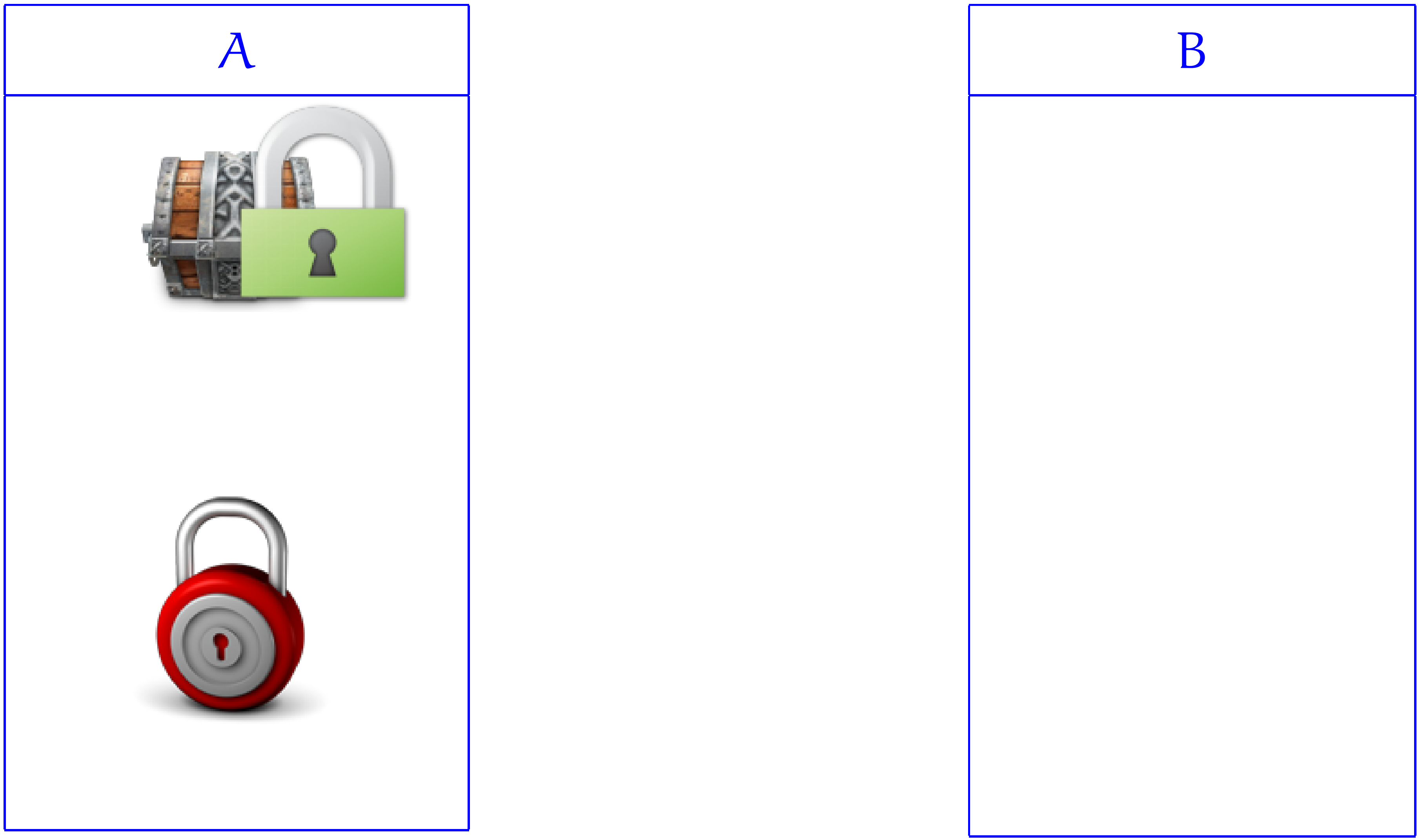
B

Key exchange

A

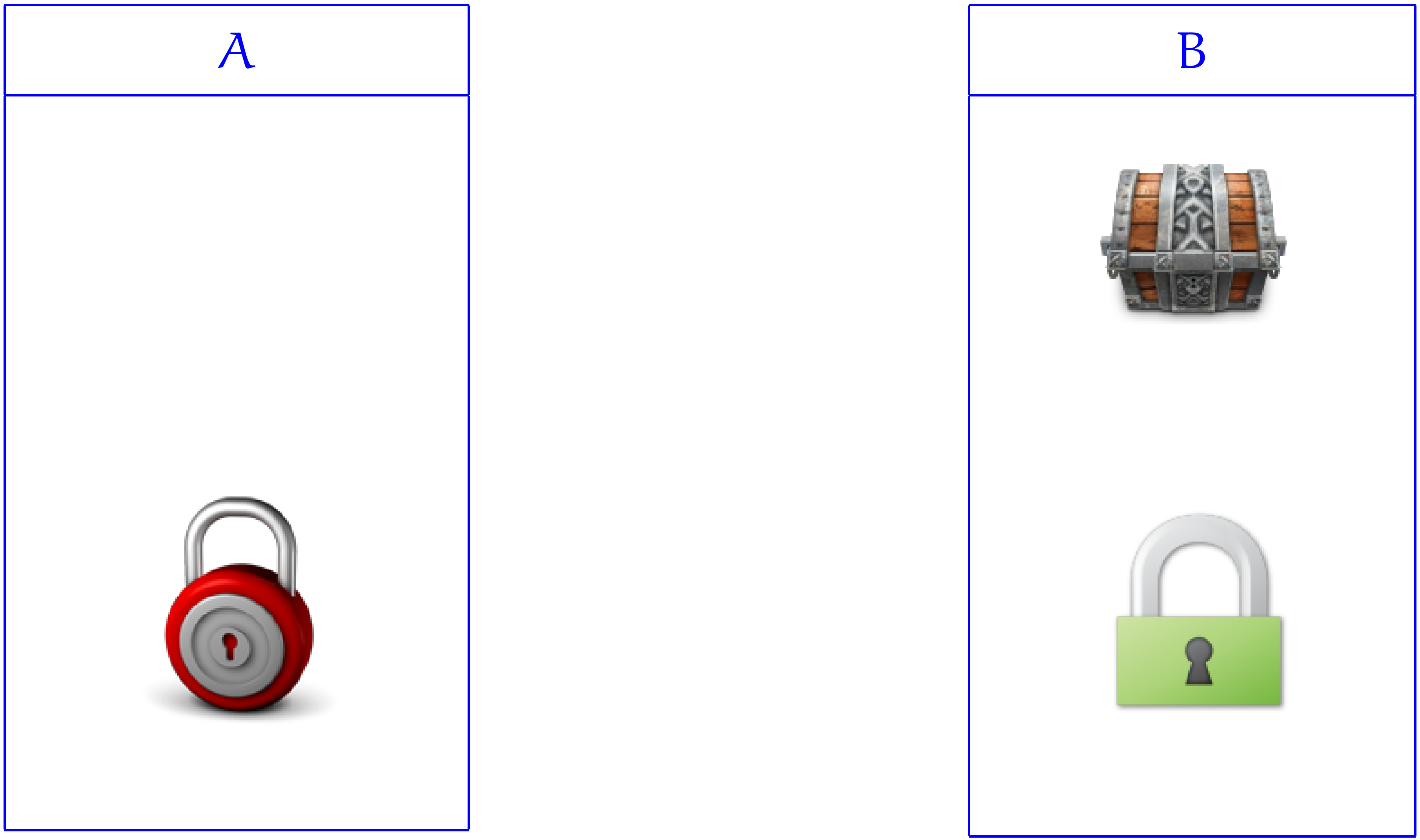
B

Key exchange



Key exchange

Key exchange



Key exchange

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

$$d = \big[\, \underbrace{lc_2(p-1, e)}_{\ell_2} \,\big]_{p-1} \ .$$

Then, for all integers k,

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

PROOF: $\exists\, \ell_1, \ell_2$

$$1 = \ell_1 (p-1) + \ell_2\, e$$

$$\forall k \quad 1 = (\ell_1 + k e) \cdot (p-1) + (\ell_2 - k(p-1)) \cdot e$$

Let k_0 be such that $\ell_2 - k_0(p-1) = d$ and define $\ell = \ell_1 + k_0 \cdot e$

$$k^{ed}$$

$$\|$$

$$k^{1+(-\ell)(p-1)}$$

$$\|$$

$$k \cdot \left(k^{(p-1)}\right)^{-\ell} \equiv k \cdot 1^{(-\ell)} \equiv k \pmod{p}$$

FLT

for k not a multiple of p

NB $1 = \ell \cdot (p-1) + d \cdot e$

$$d \cdot e = 1 - \ell (p-1)$$

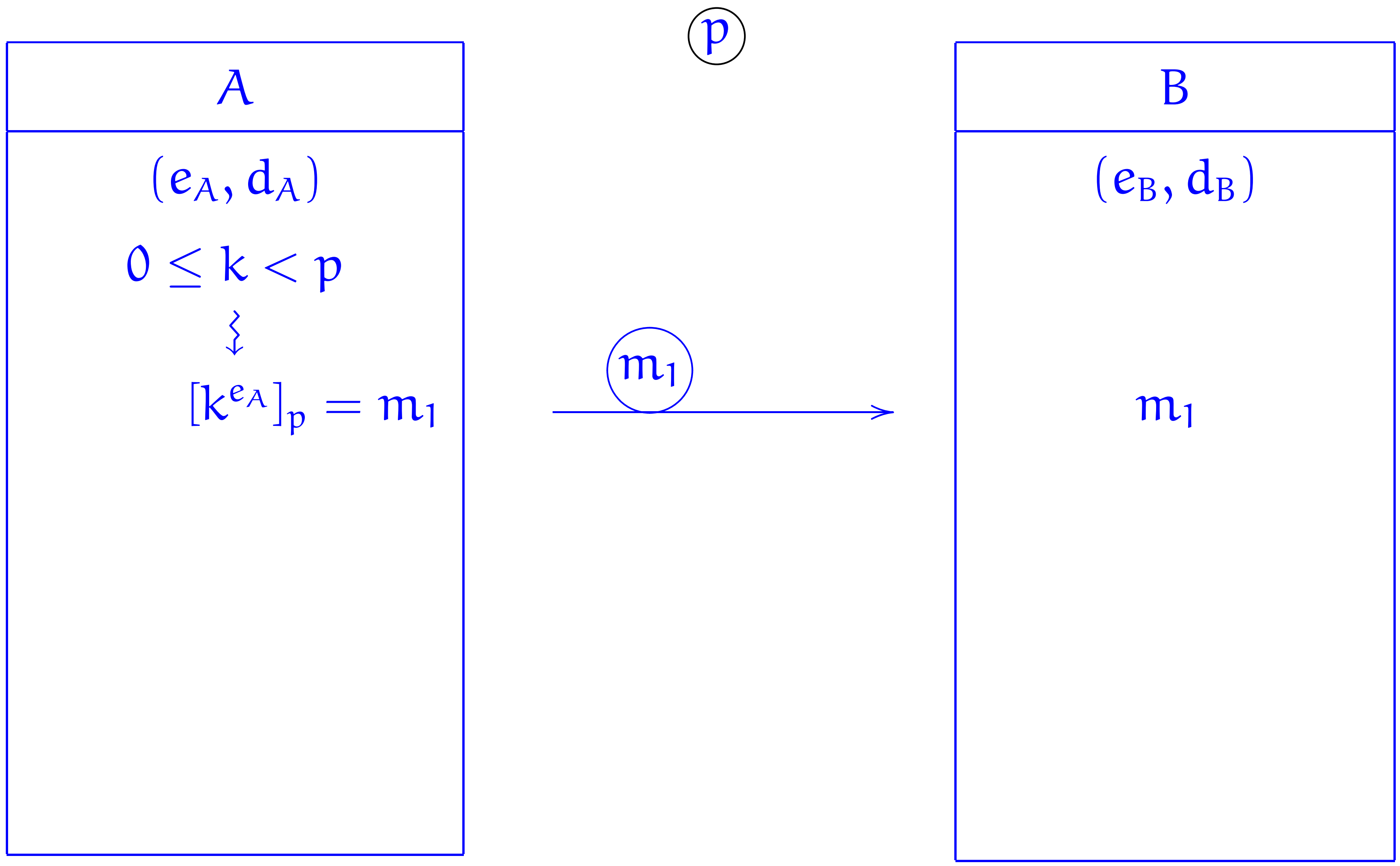
where $\ell \leq 0$

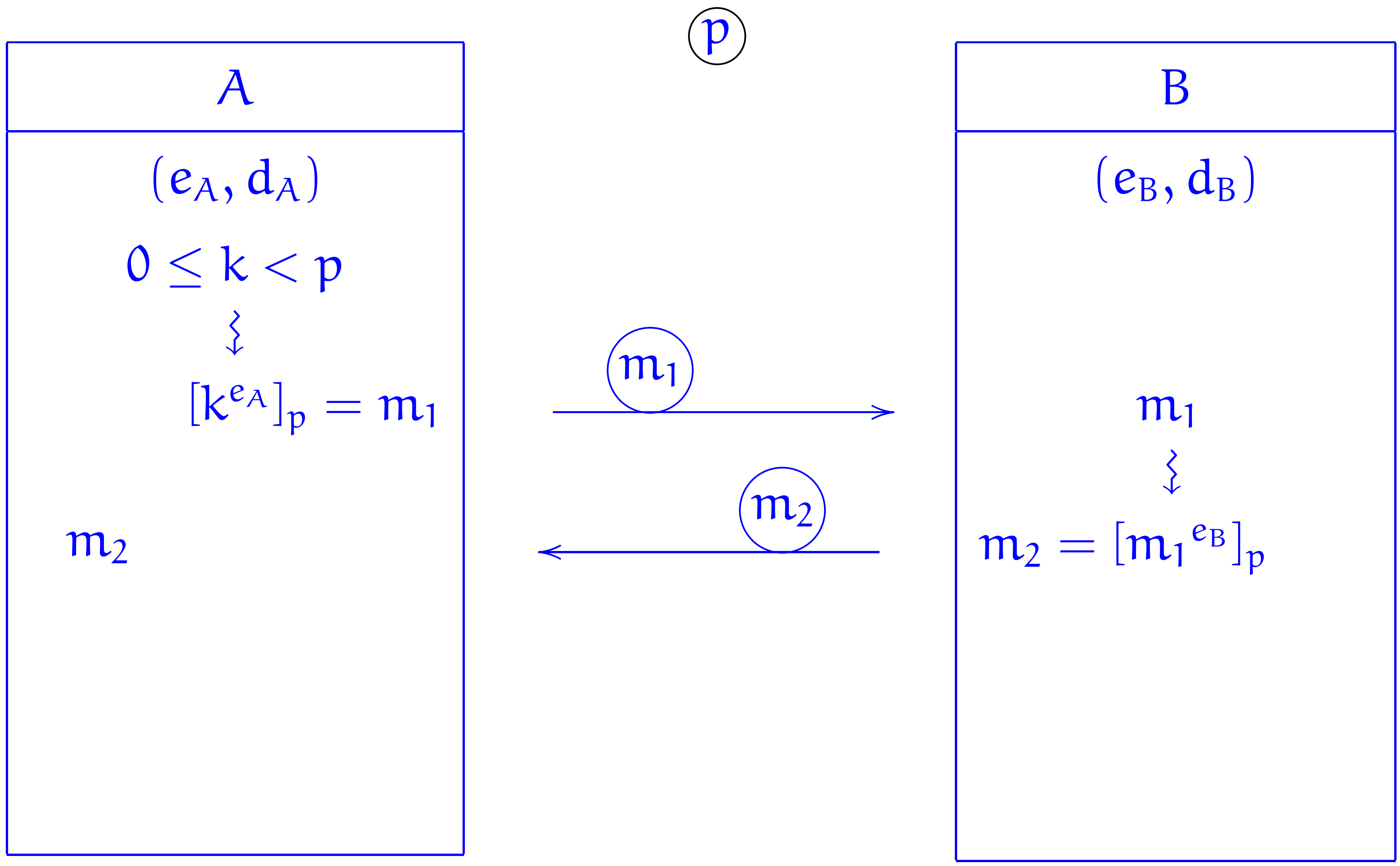
A

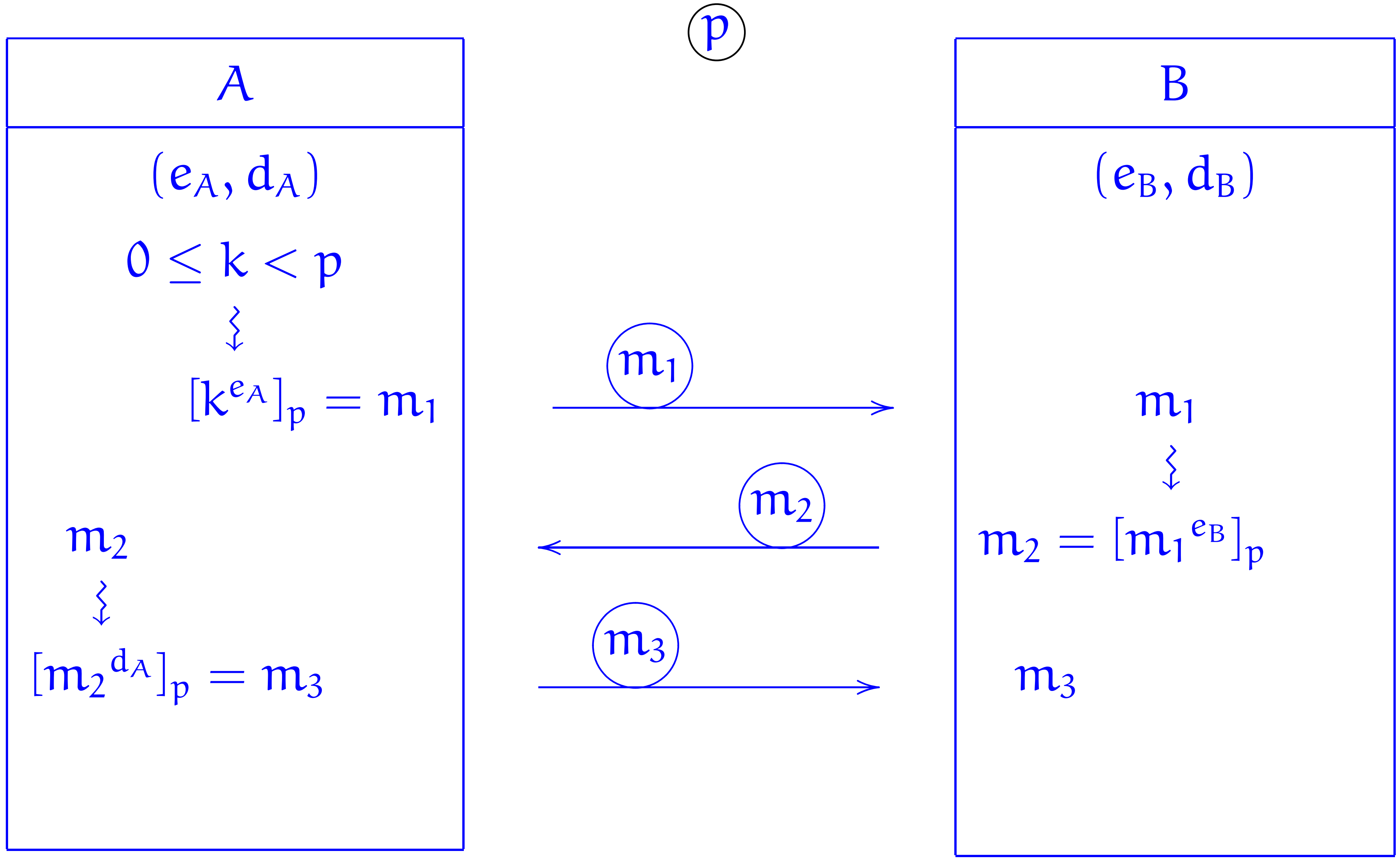
B

p

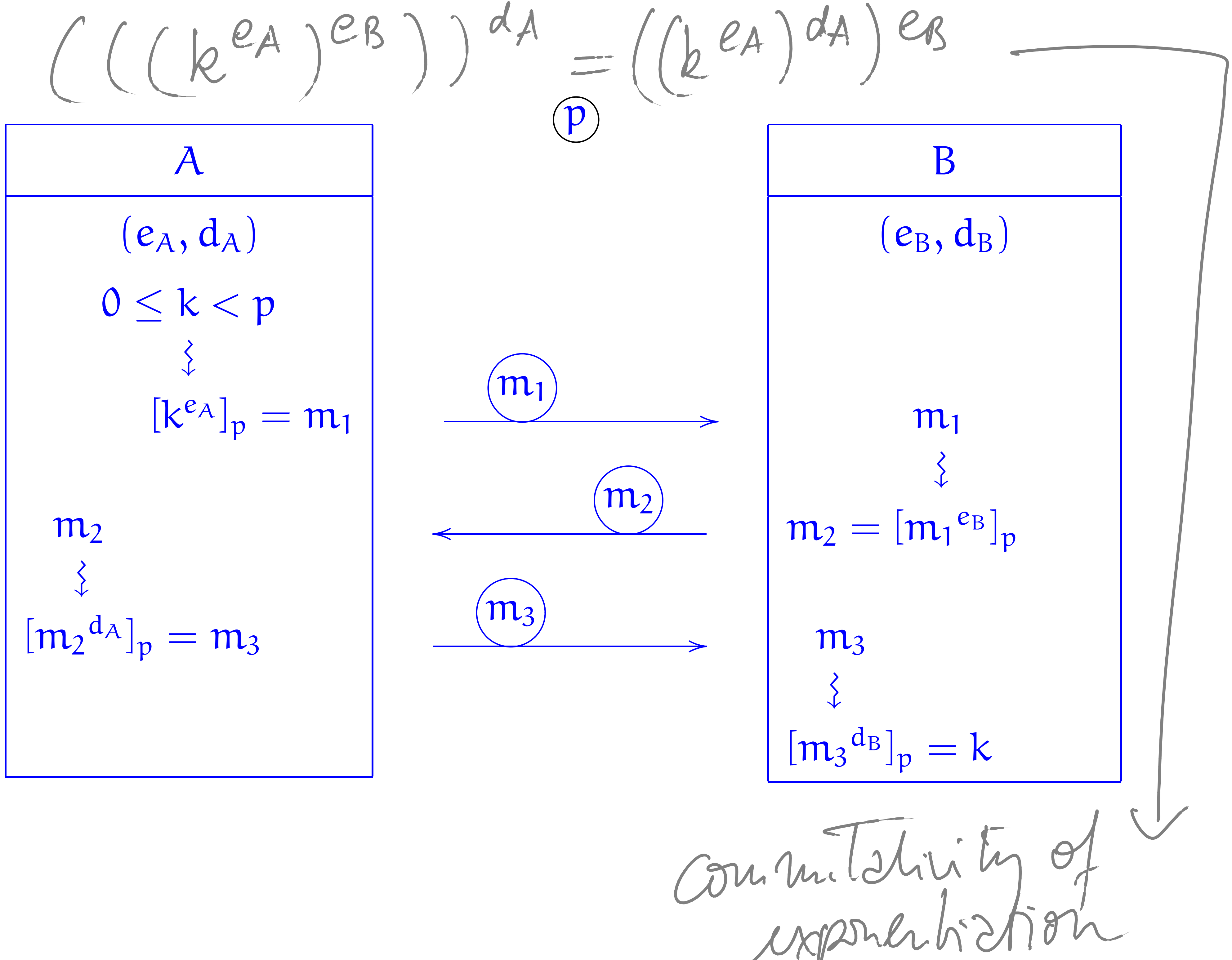
A	B
(e_A, d_A)	(e_B, d_B)
$0 \leq k < p$	


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


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
$m_2 = [m_1{}^{e_B}]_p$
m_2



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


$(((k^{e_A})^{e_B}))^{d_A} = ((k^{e_A})^{d_A})^{e_B}$
p
A
(e_A, d_A)
$0 \le k < p$
$[k^{e_A}]_p = m_1$
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
$[m_3^{d_B}]_p = k$
commutativity of exponentiation