Corollary 58 (Euclid's Theorem) *For positive integers* m *and* n*, and prime* p*, if* $p \mid (m \cdot n)$ *then* $p \mid m$ *or* $p \mid n$*.*

Now, the second part of Fermat's Little Theorem follows as a corollary of the first part and Euclid's Theorem.

PROOF: $i^{p-1} \equiv 1 \pmod{p}$ for prime p and $p \nmid i$ (1)

Know

$i^p \equiv i \pmod{p} \Rightarrow i^p - i = k \cdot p \quad \exists k$ (2)

$i^p - i = i \cdot (i^{p-1} - 1)$

From (1) and (2) by Euclid's Theorem, we have

$p \mid i^{p-1} - 1$

□

*correction

Fields of modular arithmetic

$[i^{p-2}]_p$ ✓

Corollary 59 *For prime* p*, every non-zero element* i *of* $\mathbb{Z}_\mathrm{p}$ *has as multiplicative inverse. Hence,* $\mathbb{Z}_\mathrm{p}$ *is what in the mathematical jargon is referred to as a* field.

Because $i \cdot [i^{p-2}]_p \equiv i \cdot i^{p-2} = i^{p-1} \equiv 1 \pmod{p}$

Extended Euclid's Algorithm

Example 60 ($\mathrm{egcd}(34, 13) = ((5, -13), 1)$)

	$\gcd(34, 13)$	34	$=$	$2\cdot$	13	$+$	8	8	$=$	34	$-2\cdot$	13
$=$	$\gcd(13, 8)$	13	$=$	$1\cdot$	8	$+$	5	5	$=$	13	$-1\cdot$	8
$=$	$\gcd(8, 5)$	8	$=$	$1\cdot$	5	$+$	3	3	$=$	8	$-1\cdot$	5
$=$	$\gcd(5, 3)$	5	$=$	$1\cdot$	3	$+$	2	2	$=$	5	$-1\cdot$	3
$=$	$\gcd(3, 2)$	3	$=$	$1\cdot$	2	$+$	1	1	$=$	3	$-1\cdot$	2
$=$	$\gcd(2, 1)$	2	$=$	$2\cdot$	1	$+$	0					
$=$	1											

$\gcd(m,n) = s \cdot m + t \cdot n \quad \exists s, t$ integers

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

Linear combinations

Definition 61 *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*
>
> $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \;;$$
>
> *that is*
>
> $$s \cdot m + t \cdot n = r \;.$$

Theorem 62 *For all positive integers* m *and* n*,*

1. $\gcd(m, n)$ *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*

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

can be efficiently computed.

Proposition 63 *For all integers* m *and* n,

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

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

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

   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,

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

gcd

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

egcd

```
fun egcd( m , n )
= let
    fun egcditer( ((s1,t1),r1) , lc as ((s2,t2),r2) )
    = let
        val (r,q) = 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 ) ) )
```

$gcd(m,n) = lc_1(m,n) \cdot m + lc_2(m,n) \cdot n$

$\Rightarrow n \cdot lc_2(m,n) - gcd(m,n) = lc_1(m,n) \cdot n$ □

Multiplicative inverses in modular arithmetic

Corollary 65 *For all positive integers* m *and* n,

1. $n \cdot lc_2(m,n) \equiv gcd(m,n) \pmod{m}$, *and*
2. *whenever* $gcd(m,n) = 1$,

   $[lc_2(m,n)]_m$ *is the multiplicative inverse of* $[n]_m$ *in* ~~$\mathbb{Z}_n$~~ $\mathbb{Z}_m$.

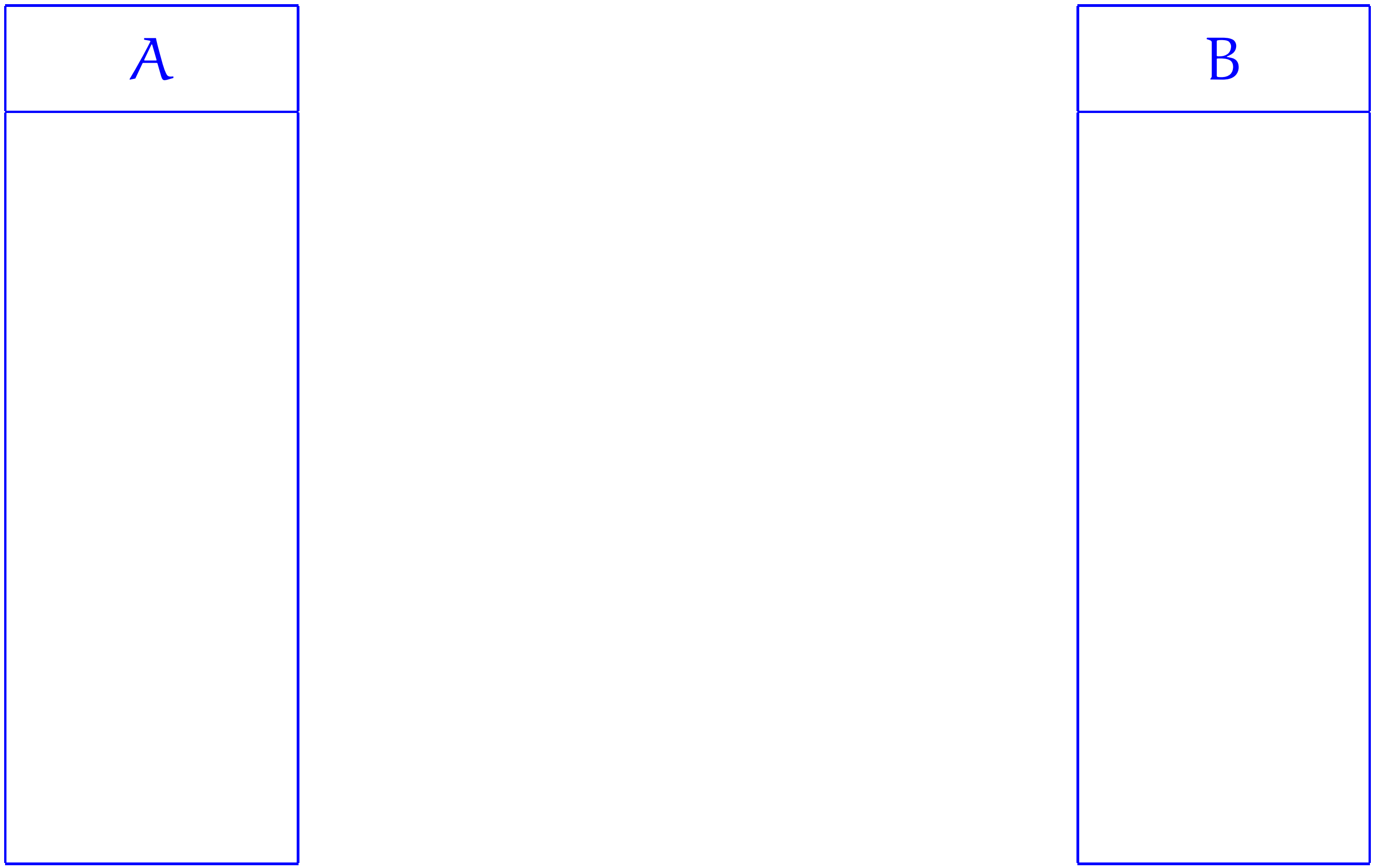
$\Rightarrow n \cdot lc_2(m,n) \equiv 1 \pmod{m}$

$\Rightarrow [n]_m \cdot [lc_2(m,n)]_m = 1 \pmod{m}$

* correction

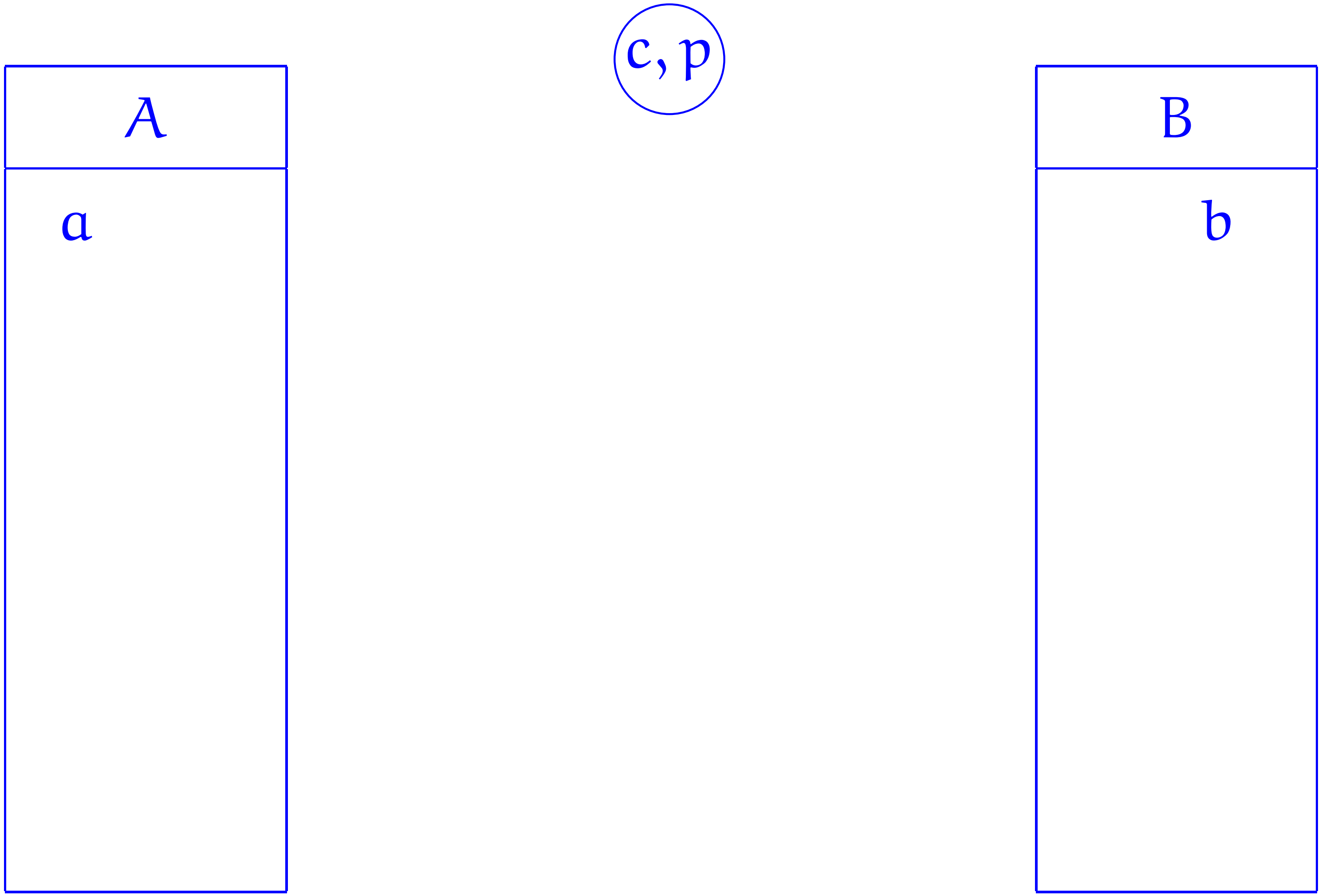
Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

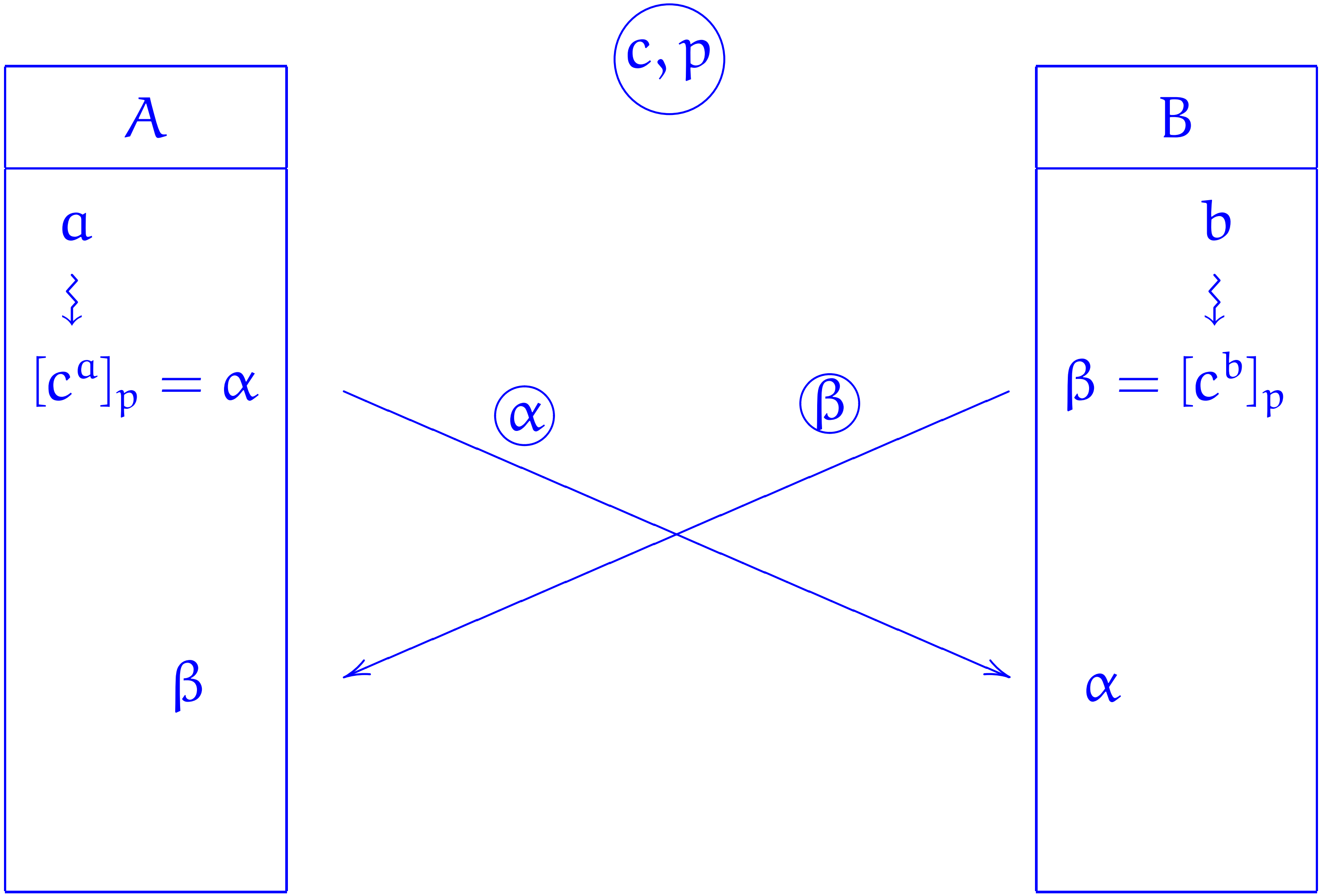
Shared secret key

c, p

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

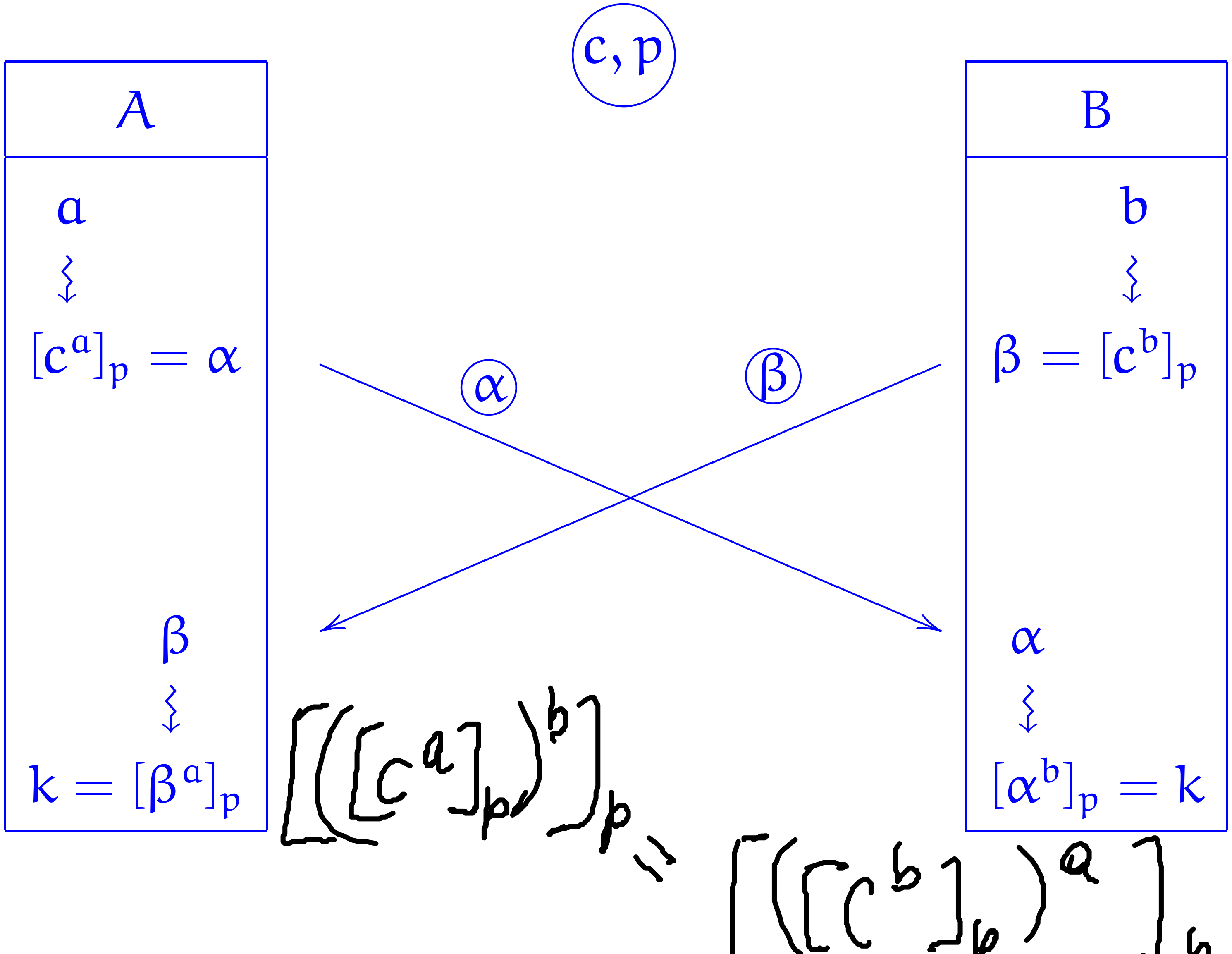
Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

Shared secret key



In the integer case

$$c$$

$$c^a = \alpha \qquad \beta = c^b$$

$$a = \log_c \alpha$$

$$\beta^a = k$$

In the modular integer case we need compute discrete logs which is hard.

Key exchange

Lemma 66 *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*,*

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

PROOF:

$$1 = \underline{lc_1}(p-1,e)\cdot(p-1) + \underline{lc_2}(p-1,e)\cdot e$$

$$= \underline{lc_1}\cdot(p-1) + \underline{lc_2}\cdot e \qquad \text{[Abbr. notation]}$$

$$= \underbrace{(\underline{lc_1} + h\cdot e)}_{l_1 \le 0}(p-1) + \underbrace{(\underline{lc_2} - h(p-1))}_{l_2 \ge 0}\cdot e \qquad \text{for some } h$$

$$d = [\underline{lc_2}]_{p-1} = [l_2]_{p-1} = \underline{rem}(l_2, p-1)$$

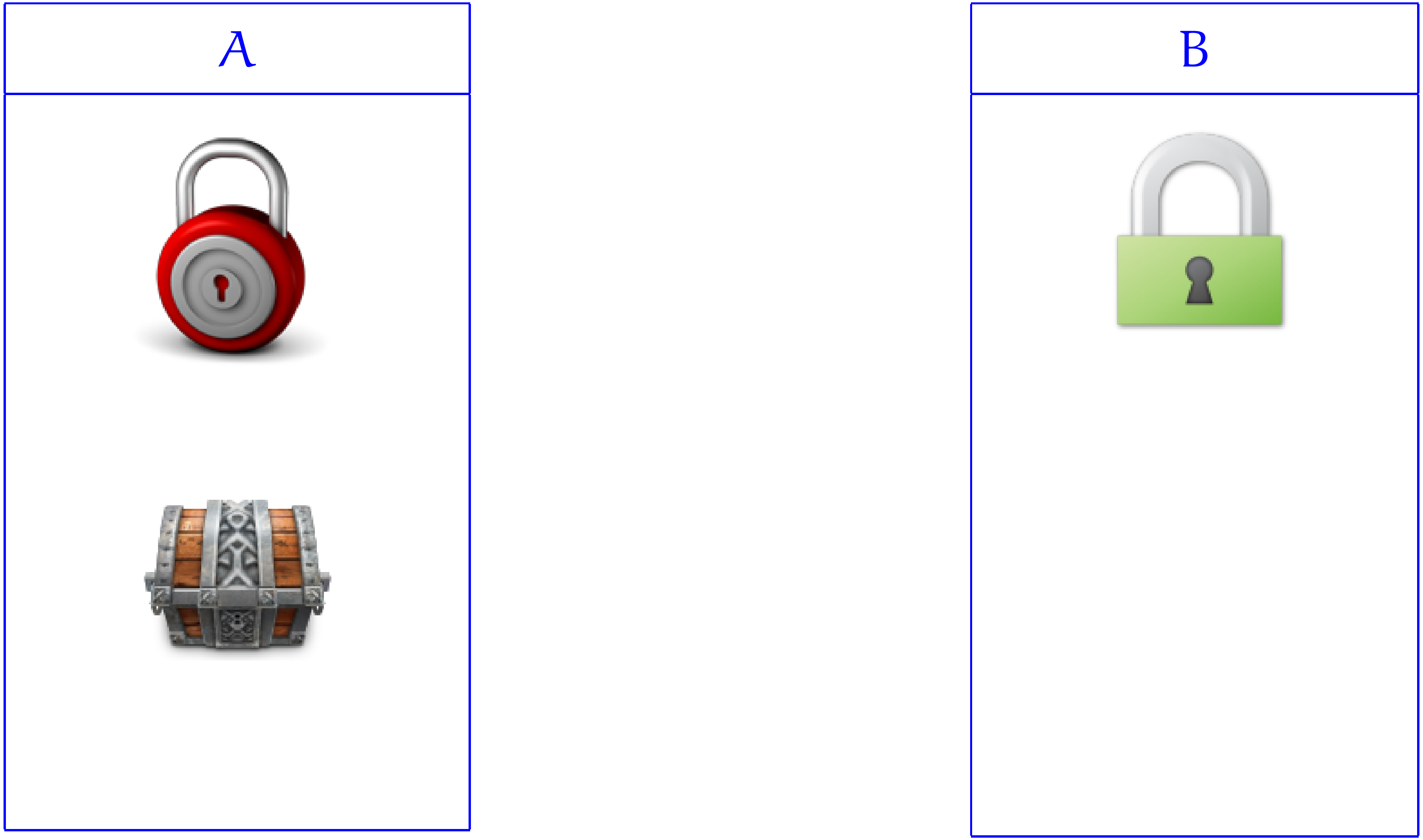
$$(k^e)^d = k^{e\cdot d} \equiv k^{1-l_1\cdot(p-1)} = k\cdot\left(k^{p-1}\right)^{l_1} \equiv k \quad \text{if } p \nmid k$$

$$k^{e\cdot d} \equiv k^{e\cdot l_2} = k^{1-l_1\cdot(p-1)}$$

see next page

$\exists q .\ l_2 = q \cdot (p-1) + d$

$$\Rightarrow x^{l_2} = \left(x^{(p-1)}\right)^q \cdot x^d \equiv \begin{cases} x^d & p \nmid x \\ 0 \equiv x^d & p \mid x \end{cases}$$


A
B

A

B

A

B

A		B
		

A	B
	

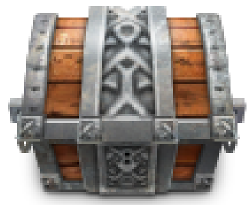
A

B

A	B
	

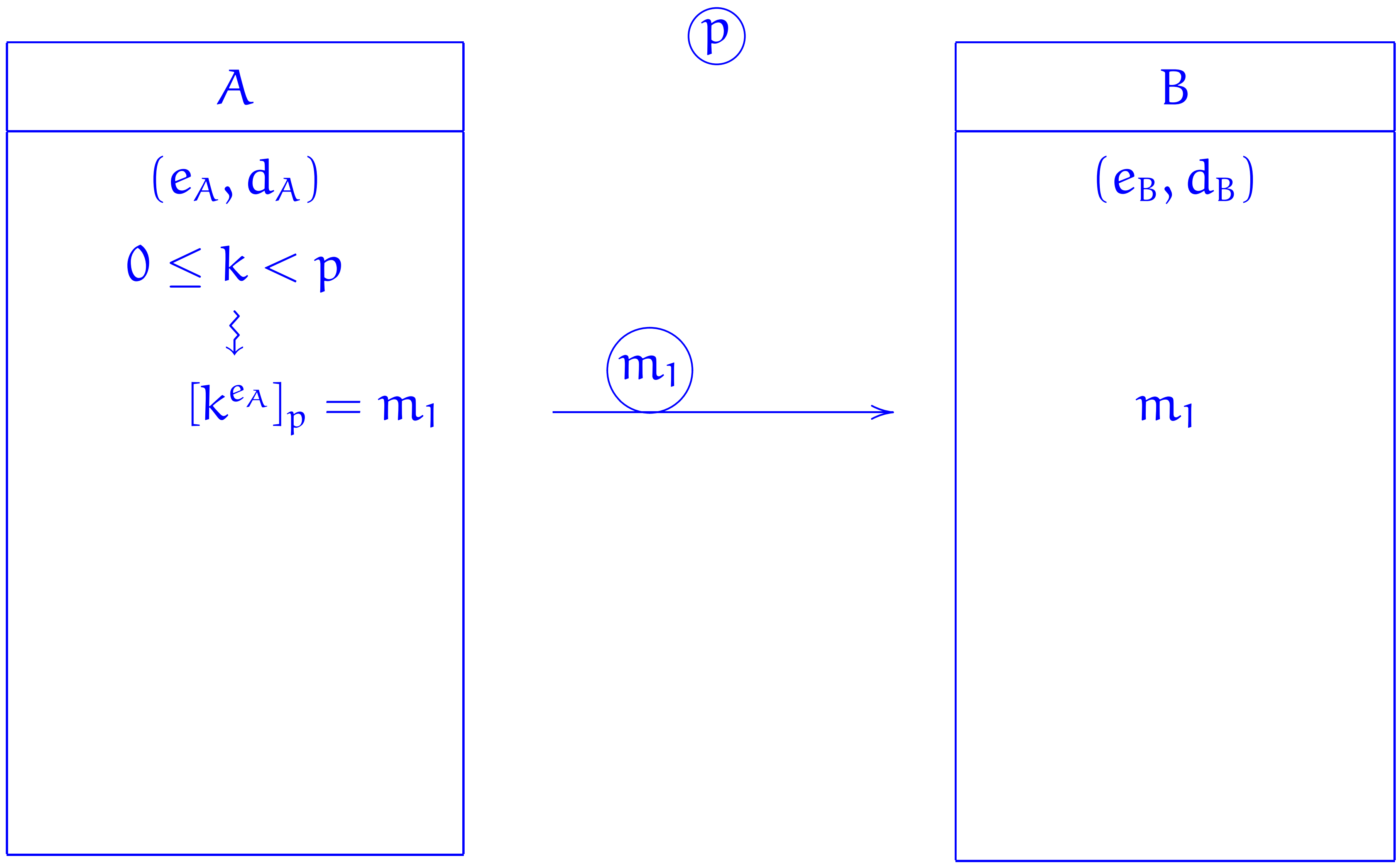
A

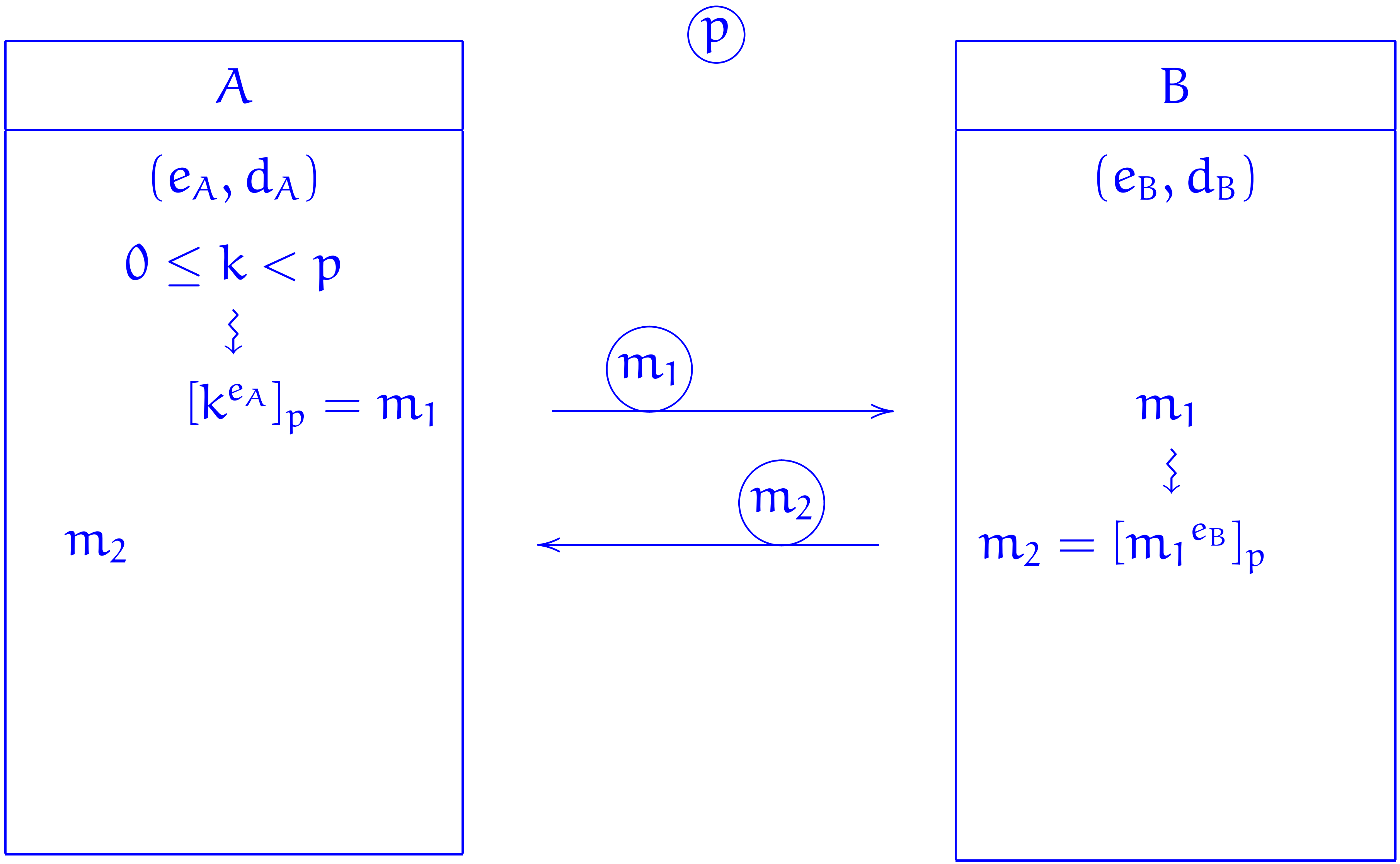
B

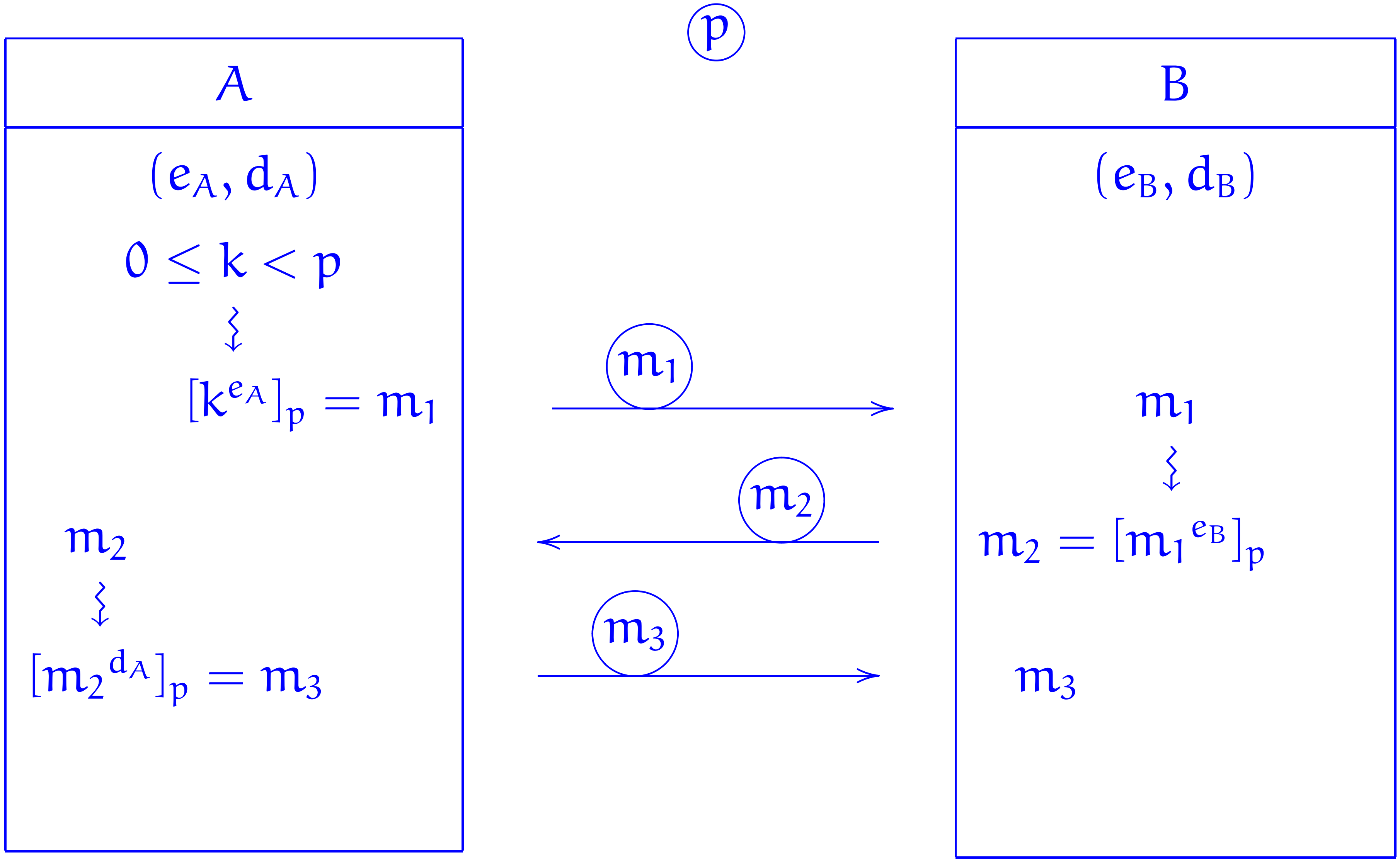


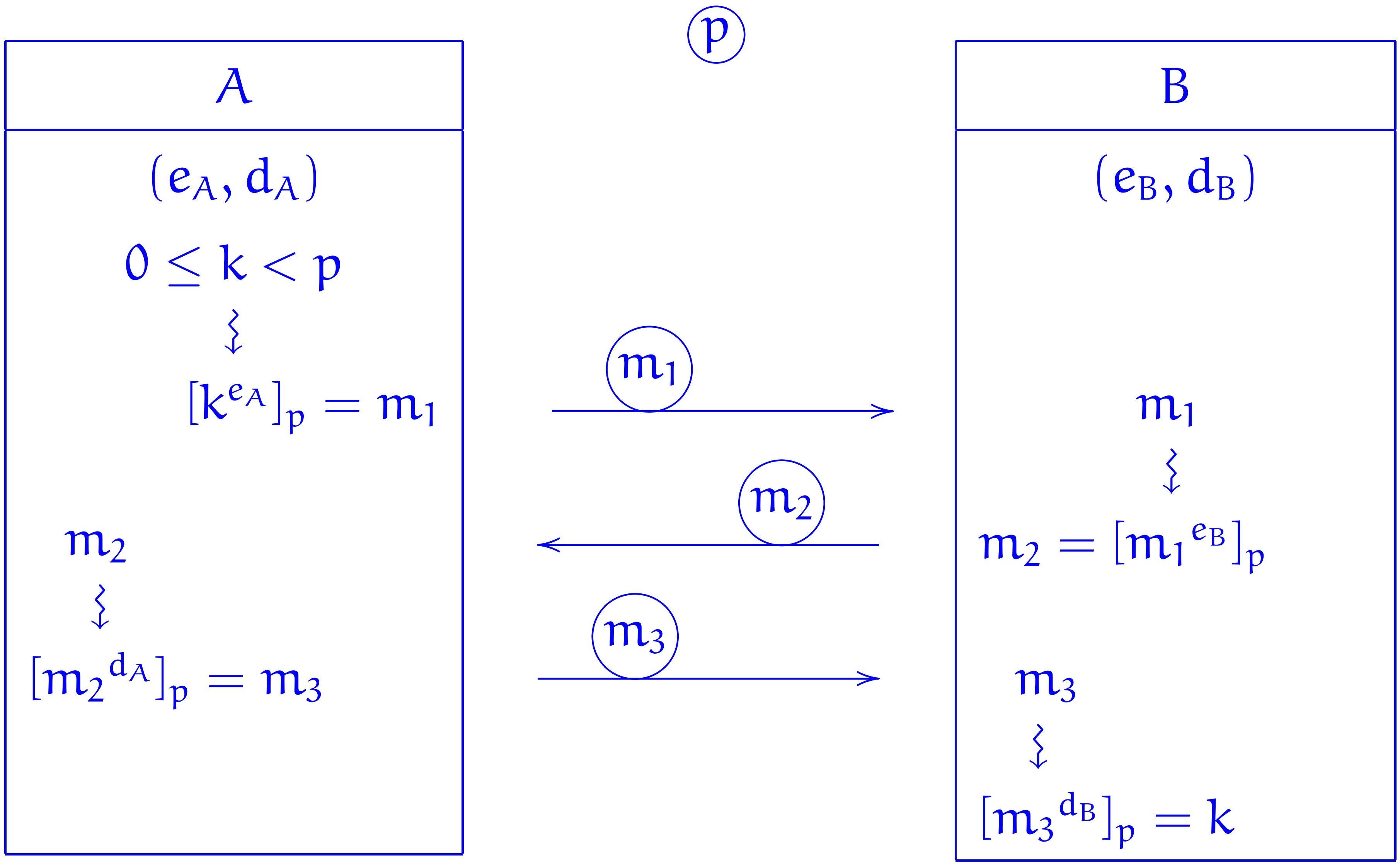
(p)

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


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


p
A
B
(eA, dA)
0 ≤ k < p
[k^eA]p = m1
m1
m2
m2
(eB, dB)
m1
m2 = [m1^eB]p
m2


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


p
A
B
(e_A, d_A)
0 ≤ 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
[m_3^{d_B}]_p = k