Euclid's Theorem

Theorem 62 *For positive integers* k, m, *and* n, *if* $k \mid (m \cdot n)$ *and* $\gcd(k, m) = 1$ *then* $k \mid n$.

PROOF:

Corollary 63 (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:

Fields of modular arithmetic

Corollary 64 *For prime p, every non-zero element i of $\mathbb{Z}_p$ has $[i^{p-2}]_p$ as multiplicative inverse. Hence, $\mathbb{Z}_p$ is what in the mathematical jargon is referred to as a* field*.*

Extended Euclid's Algorithm

Example 65 ($\mathtt{egcd}(34, 13) = \big((5, -13), 1\big)$)

$$\begin{array}{rl||rcrrcr||}
 & \gcd(34, 13) & 34 & = & 2\cdot & 13 & + & 8 \\
= & \gcd(13, 8) & 13 & = & 1\cdot & 8 & + & 5 \\
= & \gcd(8, 5) & 8 & = & 1\cdot & 5 & + & 3 \\
= & \gcd(5, 3) & 5 & = & 1\cdot & 3 & + & 2 \\
= & \gcd(3, 2) & 3 & = & 1\cdot & 2 & + & 1 \\
= & \gcd(2, 1) & 2 & = & 2\cdot & 1 & + & \multicolumn{1}{r}{0} \\
= & \multicolumn{1}{l}{1} & \multicolumn{6}{l}{}
\end{array}$$

Extended Euclid's Algorithm

Example 65 ($\texttt{egcd}(34, 13) = \big((5, -13), 1\big)$**)**

$$\begin{array}{rl||rcrrcr||rcrrr}
 & \gcd(34, 13) & 34 & = & 2\cdot & 13 & + & 8 & 8 & = & 34 & -2\cdot & 13 \\
= & \gcd(13, 8) & 13 & = & 1\cdot & 8 & + & 5 & 5 & = & 13 & -1\cdot & 8 \\
= & \gcd(8, 5) & 8 & = & 1\cdot & 5 & + & 3 & 3 & = & 8 & -1\cdot & 5 \\
= & \gcd(5, 3) & 5 & = & 1\cdot & 3 & + & 2 & 2 & = & 5 & -1\cdot & 3 \\
= & \gcd(3, 2) & 3 & = & 1\cdot & 2 & + & 1 & 1 & = & 3 & -1\cdot & 2 \\
= & \gcd(2, 1) & 2 & = & 2\cdot & 1 & + & 0 & & & & & \\
= & 1 & & & & & & & & & & &
\end{array}$$

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

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

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

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

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

Linear combinations

Definition 66 *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*
>
> $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \quad ;$$
>
> *that is*
>
> $$s \cdot m + t \cdot n = r \quad .$$

Theorem 67 *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*

$$\left[\begin{array}{cc} \mathrm{lc}_1(m,n) & \mathrm{lc}_2(m,n) \end{array}\right] \cdot \left[\begin{array}{c} m \\ n \end{array}\right] = \mathrm{gcd}(m,n) \quad ,$$

can be efficiently computed.

Proposition 68 *For all integers m and n,*

1. $$\left[\begin{array}{cc} 1 & 0 \end{array}\right] \cdot \left[\begin{array}{c} m \\ n \end{array}\right] = m \quad \wedge \quad \left[\begin{array}{cc} 0 & 1 \end{array}\right] \cdot \left[\begin{array}{c} m \\ n \end{array}\right] = n \quad ;$$

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

   $$\left[\begin{array}{cc} s_1 & t_1 \end{array}\right] \cdot \left[\begin{array}{c} m \\ n \end{array}\right] = r_1 \quad \wedge \quad \left[\begin{array}{cc} s_2 & t_2 \end{array}\right] \cdot \left[\begin{array}{c} m \\ n \end{array}\right] = r_2$$

   implies

   $$\left[\begin{array}{cc} s_1 + s_2 & t_1 + t_2 \end{array}\right] \cdot \left[\begin{array}{c} m \\ n \end{array}\right] = r_1 + r_2 \quad ;$$

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

   $$\left[\begin{array}{cc} s & t \end{array}\right] \cdot \left[\begin{array}{c} m \\ n \end{array}\right] = r \text{ implies } \left[\begin{array}{cc} k \cdot s & k \cdot t \end{array}\right] \cdot \left[\begin{array}{c} m \\ n \end{array}\right] = k \cdot r \quad .$$

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 ) ) )
```

Multiplicative inverses in modular arithmetic

Corollary 72 *For all positive integers* m *and* n*,*

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

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

Diffie-Hellman cryptographic method

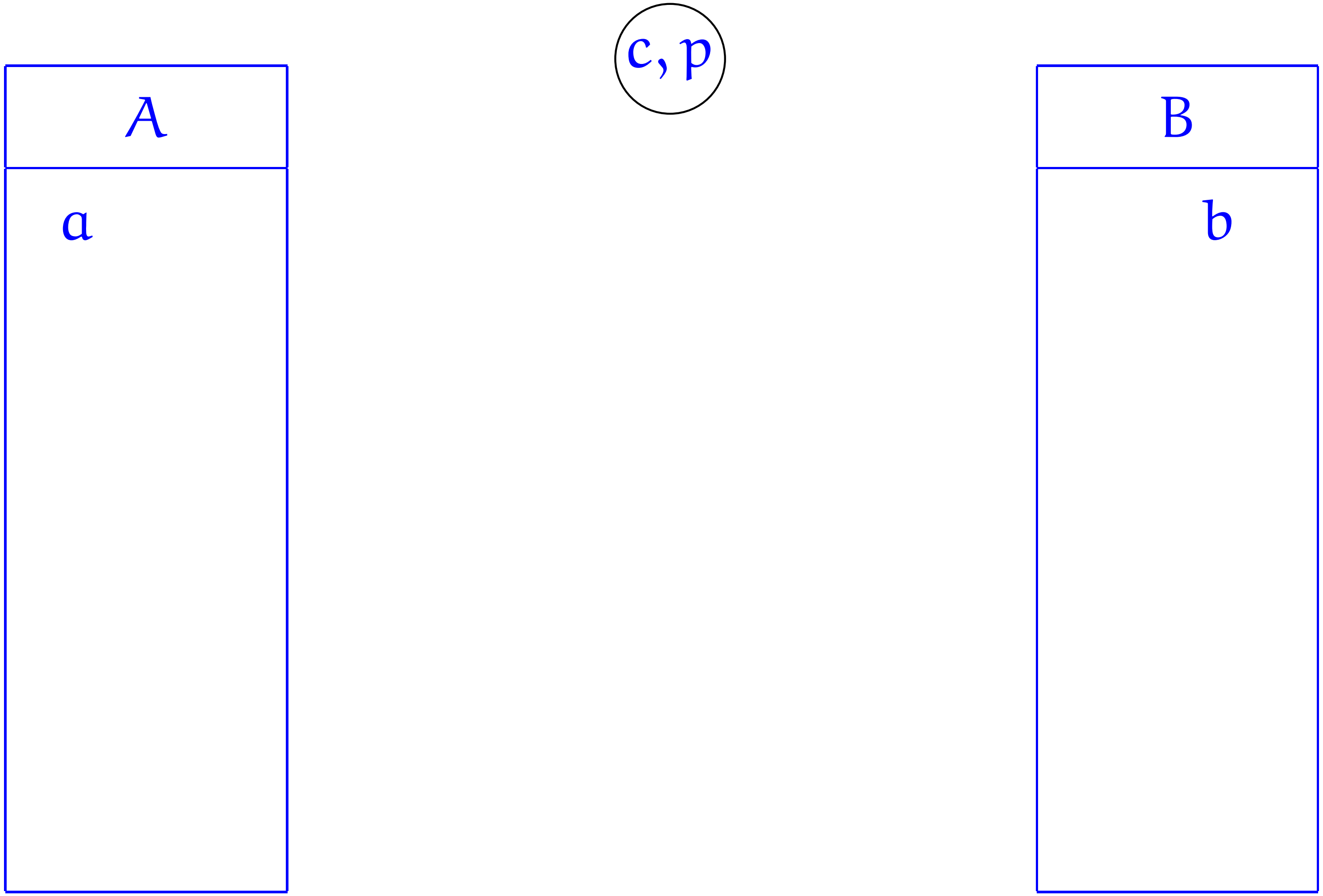
Shared secret key

A

B

Diffie-Hellman cryptographic method

Shared secret key



c, p

A

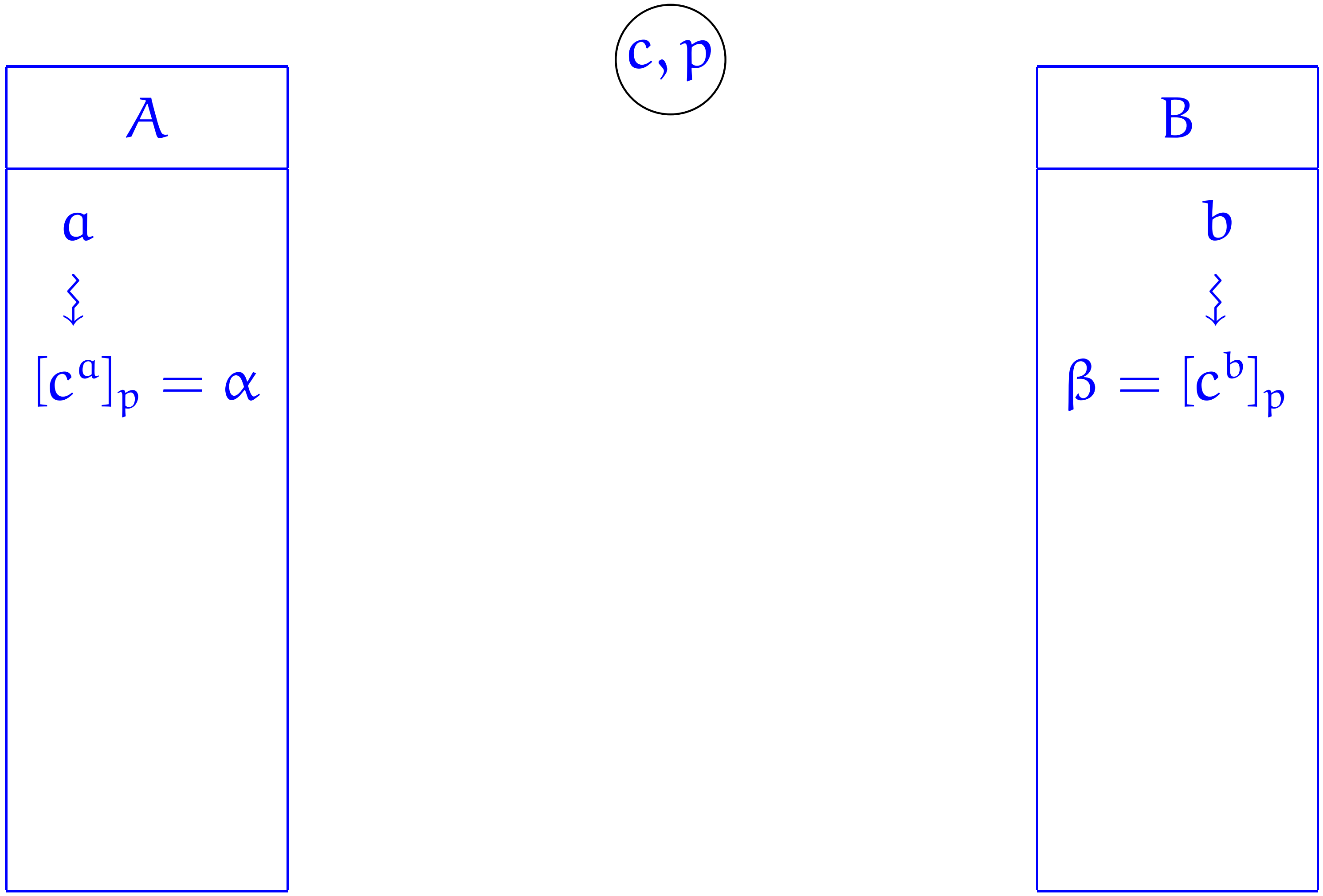
a

B

b

Diffie-Hellman cryptographic method

Shared secret key



$\boxed{c, p}$

A

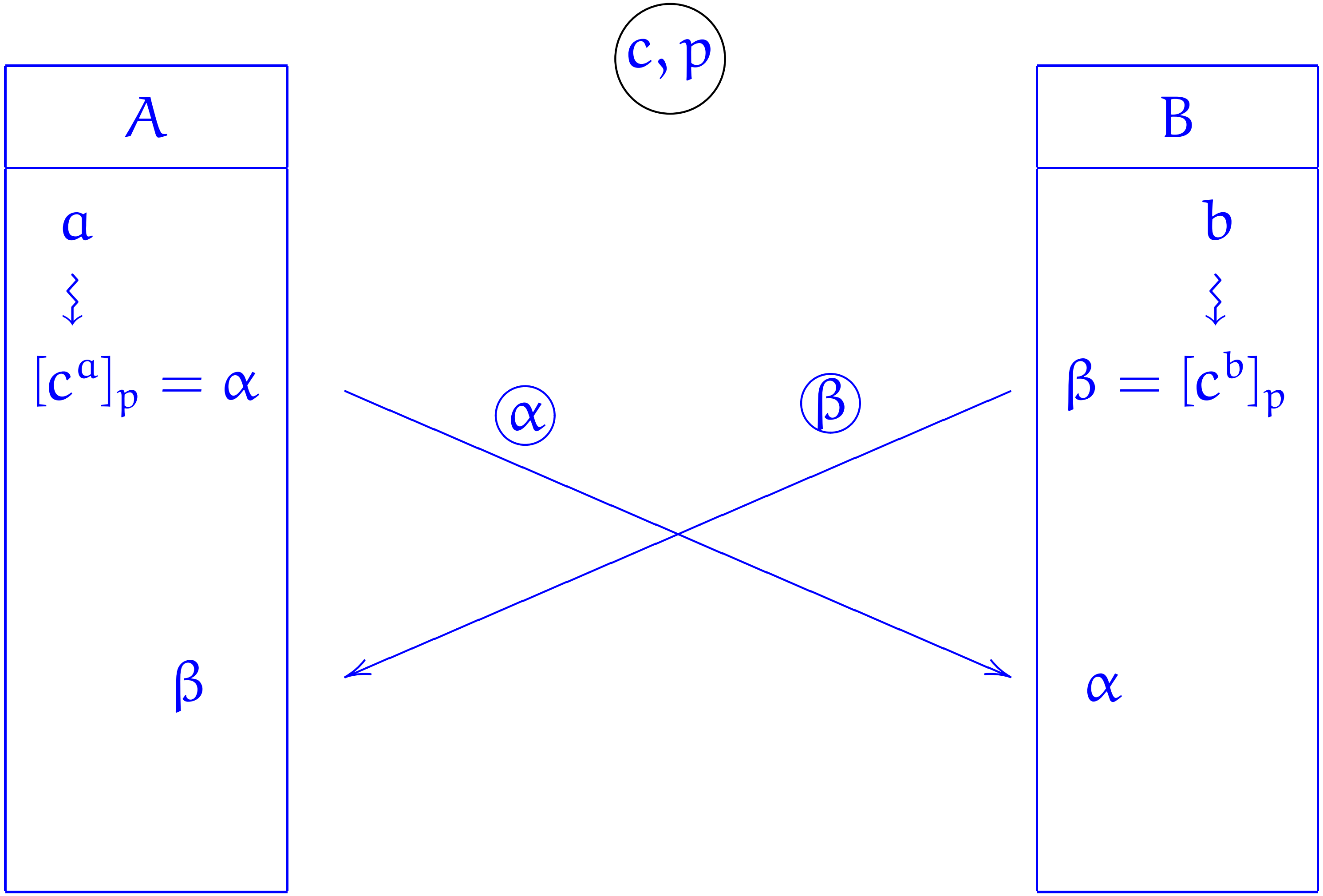
$$\begin{array}{c} a \\ \rightsquigarrow \\ [c^a]_p = \alpha \end{array}$$

B

$$\begin{array}{c} b \\ \rightsquigarrow \\ \beta = [c^b]_p \end{array}$$

Diffie-Hellman cryptographic method

Shared secret key



c, p

A

a

$[c^a]_p = \alpha$

β

B

b

$\beta = [c^b]_p$

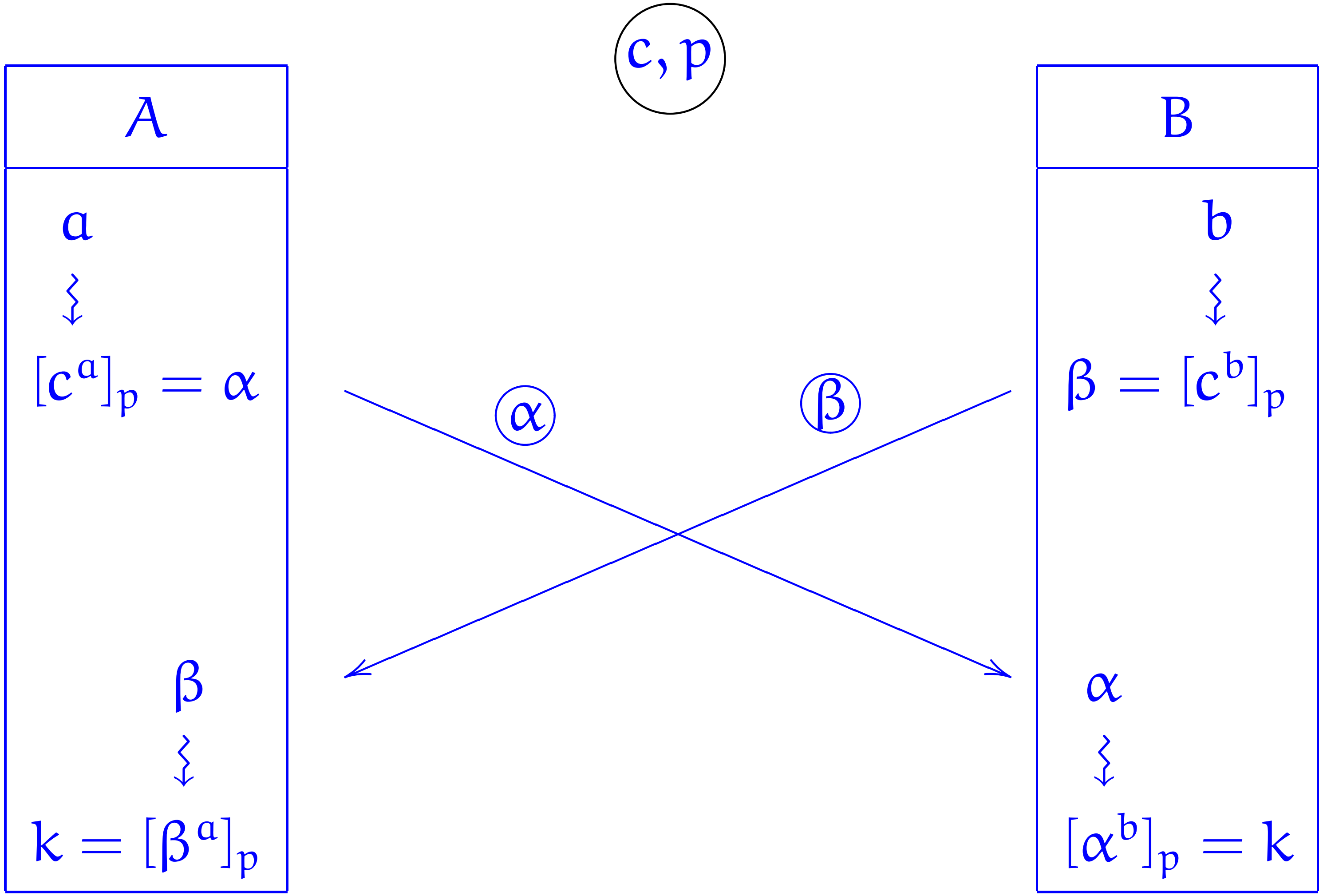
α

α

β

Diffie-Hellman cryptographic method

Shared secret key



c, p

A

a

$\downarrow$

$[c^a]_p = \alpha$

β

$\downarrow$

$k = [\beta^a]_p$

B

b

$\downarrow$

$\beta = [c^b]_p$

α

$\downarrow$

$[\alpha^b]_p = k$

Key exchange

Lemma 73 *Let* p *be a prime and* e *a positive integer with* $\gcd(p-1,e)=1$. *Define*

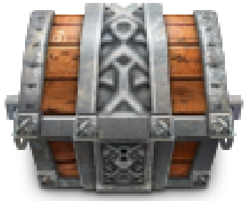
$$d = \left[\,\mathrm{lc}_2(p-1,e)\,\right]_{p-1} \quad .$$

Then, for all integers k,

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

PROOF:

A



B

A	B
	

A

B

A

B

A	B
	

A

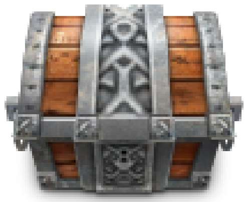
B

A

B

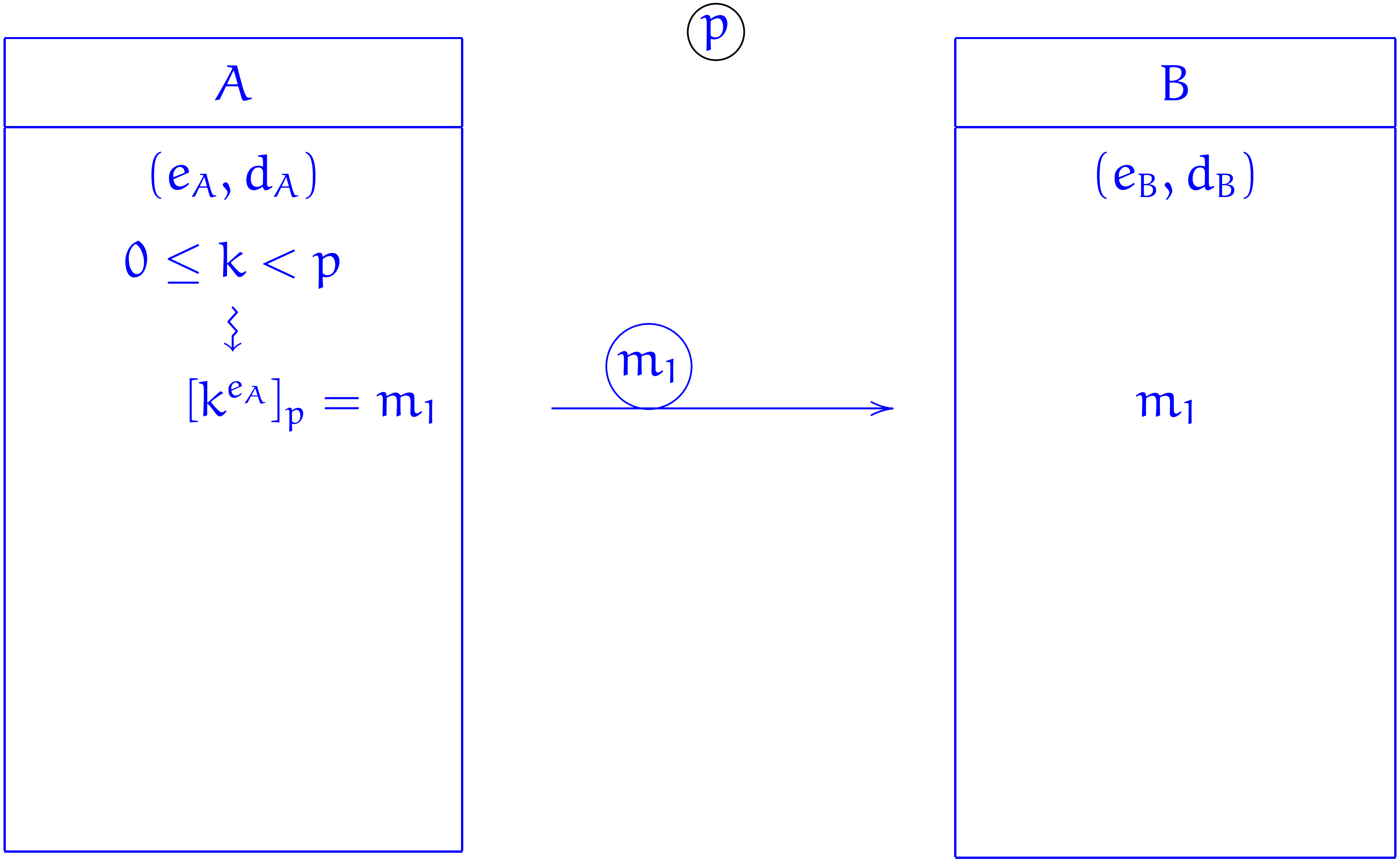
A

B



ⓟ

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



$\textcircled{p}$

A

(e_A, d_A)

$0 \le k < p$

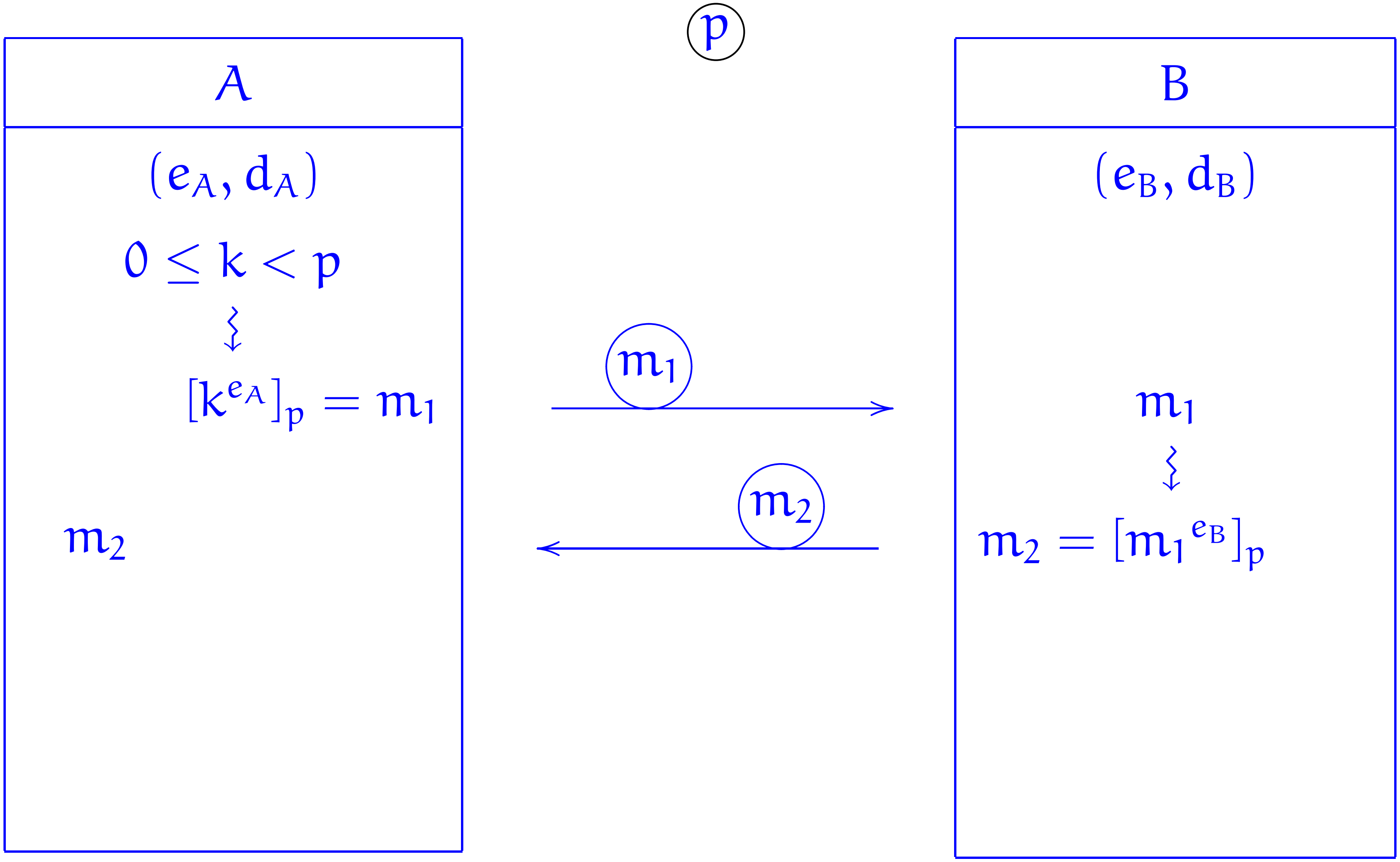
$[k^{e_A}]_p = m_1$

$\xrightarrow{\textcircled{m_1}}$

B

(e_B, d_B)

m_1



p

A

(e_A, d_A)

$0 \le k < p$

$\downarrow$

$[k^{e_A}]_p = m_1$

$\xrightarrow{m_1}$

$\xleftarrow{m_2}$

m_2

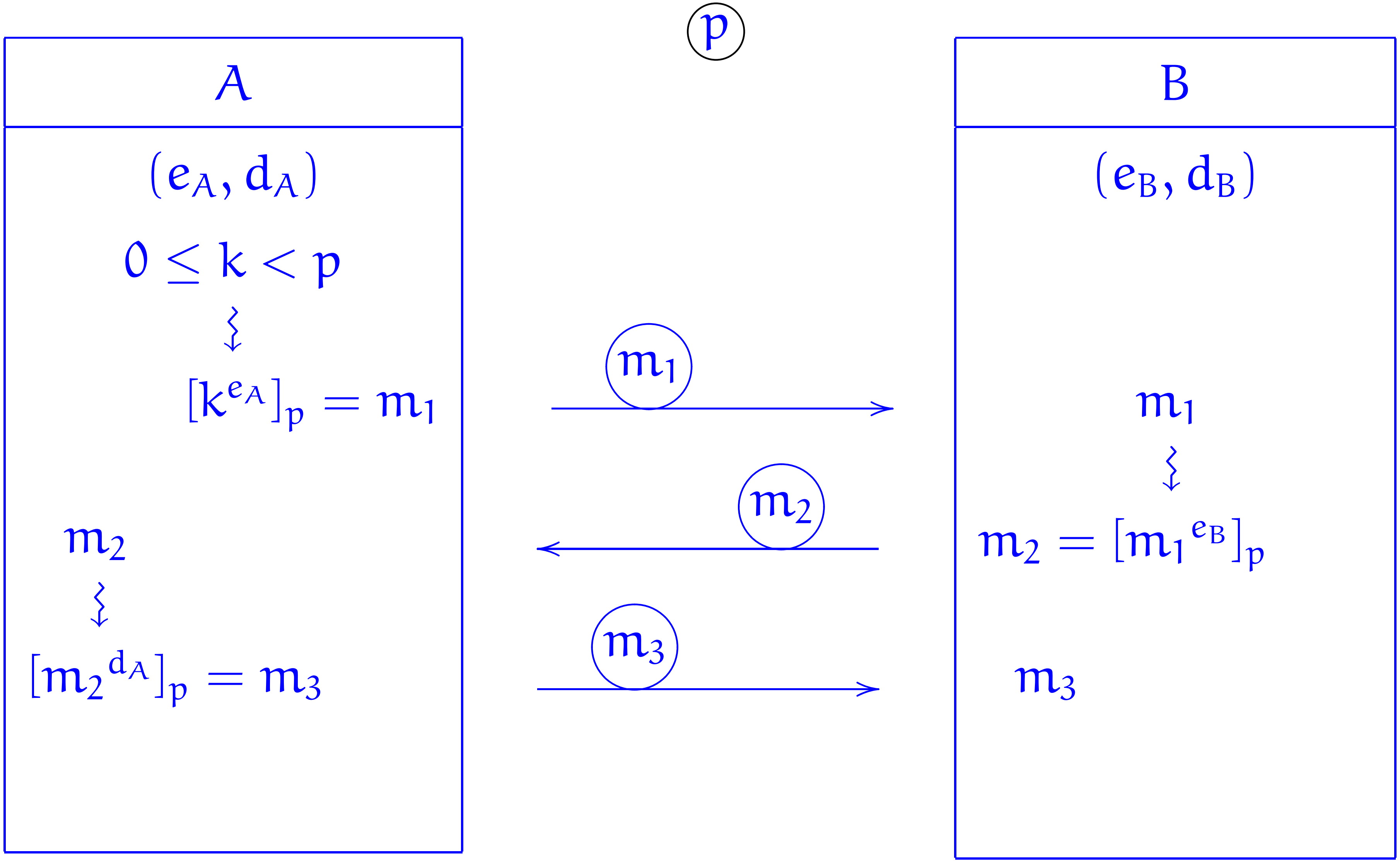
B

(e_B, d_B)

m_1

$\downarrow$

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



$\textcircled{p}$

A

(e_A, d_A)

$0 \le k < p$

$[k^{e_A}]_p = m_1$

$\xrightarrow{\;m_1\;}$

B

(e_B, d_B)

m_1

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

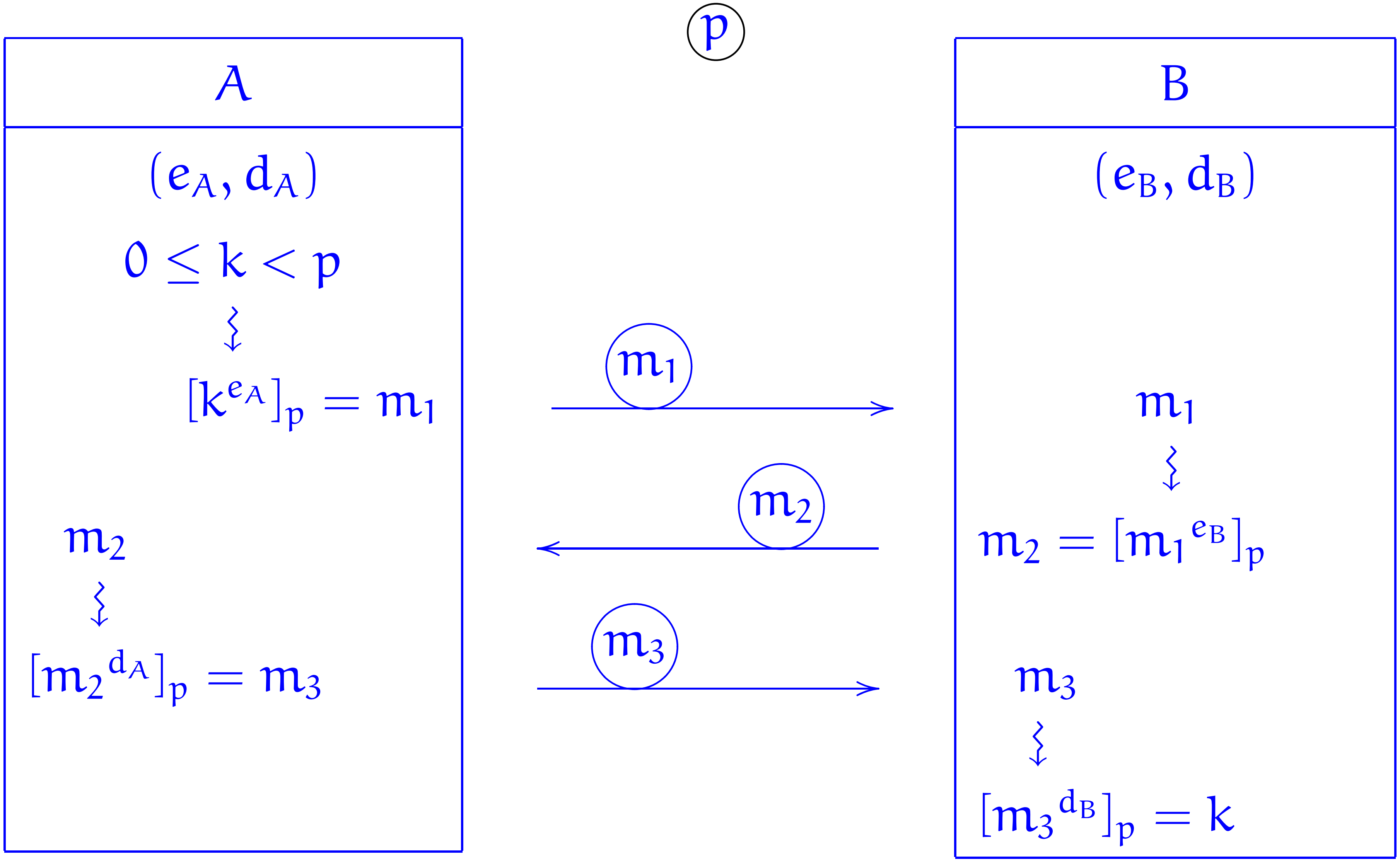
$\xleftarrow{\;m_2\;}$

m_2

$[{m_2}^{d_A}]_p = m_3$

$\xrightarrow{\;m_3\;}$

m_3



$\textcircled{p}$

A

(e_A, d_A)

$0 \leq k < p$

$\rightsquigarrow$

$[k^{e_A}]_p = m_1$

m_2

$\rightsquigarrow$

$[m_2{}^{d_A}]_p = m_3$

$\xrightarrow{\textcircled{m_1}}$

$\xleftarrow{\textcircled{m_2}}$

$\xrightarrow{\textcircled{m_3}}$

B

(e_B, d_B)

m_1

$\rightsquigarrow$

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

m_3

$\rightsquigarrow$

$[m_3{}^{d_B}]_p = k$