Exercises

(1) For positive integers ℓ, m, n,

$$\gcd(\ell m, \ell n) \mid \ell \cdot \gcd(m, n).$$

(2) For a prime p and $0 < m < p$,

$$p \mid \binom{p}{m}.$$

(1) Let l, m, n be positive integers.

RTP $\gcd(lm, ln) \mid l \cdot \gcd(m, n)$.

Note that

$l \mid lm \wedge l \mid ln \Rightarrow l \mid \gcd(lm, ln)$.

Hence $\gcd(lm, ln) = l \cdot k$ for an int. k.

Also $\gcd(lm, ln) \mid lm$ and $\gcd(lm, ln) \mid ln$

Thus $lm = \gcd(lm, ln) \cdot a = lk \cdot a$ for some int. a

and $ln = \gcd(lm, ln) \cdot b = lk \cdot b$ for some int. b.

It follows that $m = k \cdot a$ and $n = k \cdot b$.

So $k \mid m$ and $k \mid n$

and thus $k \mid \gcd(m,n)$

and further $lk \mid l \cdot \gcd(m,n)$.

so we are done. $\boxtimes$

(2) For p prime, $0 < m < p$

RTP: $p \mid \binom{p}{m}$

$$(p-m)\binom{p}{m} = p \cdot \binom{p-1}{m}$$

$$\binom{p}{m} = \frac{p}{(p-m)} \frac{(p-1)!}{m!\,(p-m-1)!}$$

$\Rightarrow$ Since $\gcd(p, p-m) = 1$

By Euclid's Thm, $p \mid \binom{p}{m}$ $\boxtimes$

Extended Euclid's Algorithm

Example 67

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

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

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

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.

NB: There is an infinite number of coefficients expressing an integer as a linear combination of other two, as for all integers s, t, m, n, r:

$$s \cdot m + t \cdot n = r$$

If

for all integers k,

$$(s+kn) \cdot m + (t-km) n = r .$$

Proposition 70 *For all integers* $\mathfrak{m}$ *and* $\mathfrak{n}$,

1. $\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} \mathfrak{m} \\ \mathfrak{n} \end{bmatrix} = \mathfrak{m} \ \wedge \ \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} \mathfrak{m} \\ \mathfrak{n} \end{bmatrix} = \mathfrak{n}$;

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

1. $\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \quad \wedge \quad \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

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

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

implies

$$\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \;;$$

$s_1 + s_2$ $t_1 + t_2$

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

1. $\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \;\wedge\; \begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;

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

$$\begin{bmatrix} ?_1 & ?_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \;;$$

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

$$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \text{ implies } \begin{bmatrix} \overset{ks}{\cancel{?_1}} & \overset{kt}{\cancel{?_2}} \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = k \cdot r \;.$$

EXTENDED EUCLID'S ALGORITHM

We extend Euclid's Algorithm $\gcd(m,n)$ from computing on pairs of positive integers to computing on pairs of triples $((s,t),r)$ with s,t integers and r a positive integer satisfying the invariant that s,t are coefficients expressing r as an integer linear combination of m and n.

gcd

```
fun  gcd( m , n )
= let
    fun  gcditer( ((s1,t1),r1) ,  c as ((s2,t2),r2) )
    = let
        val (q,r) = 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 (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 74 *For all positive integers* m *and* n*,*

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

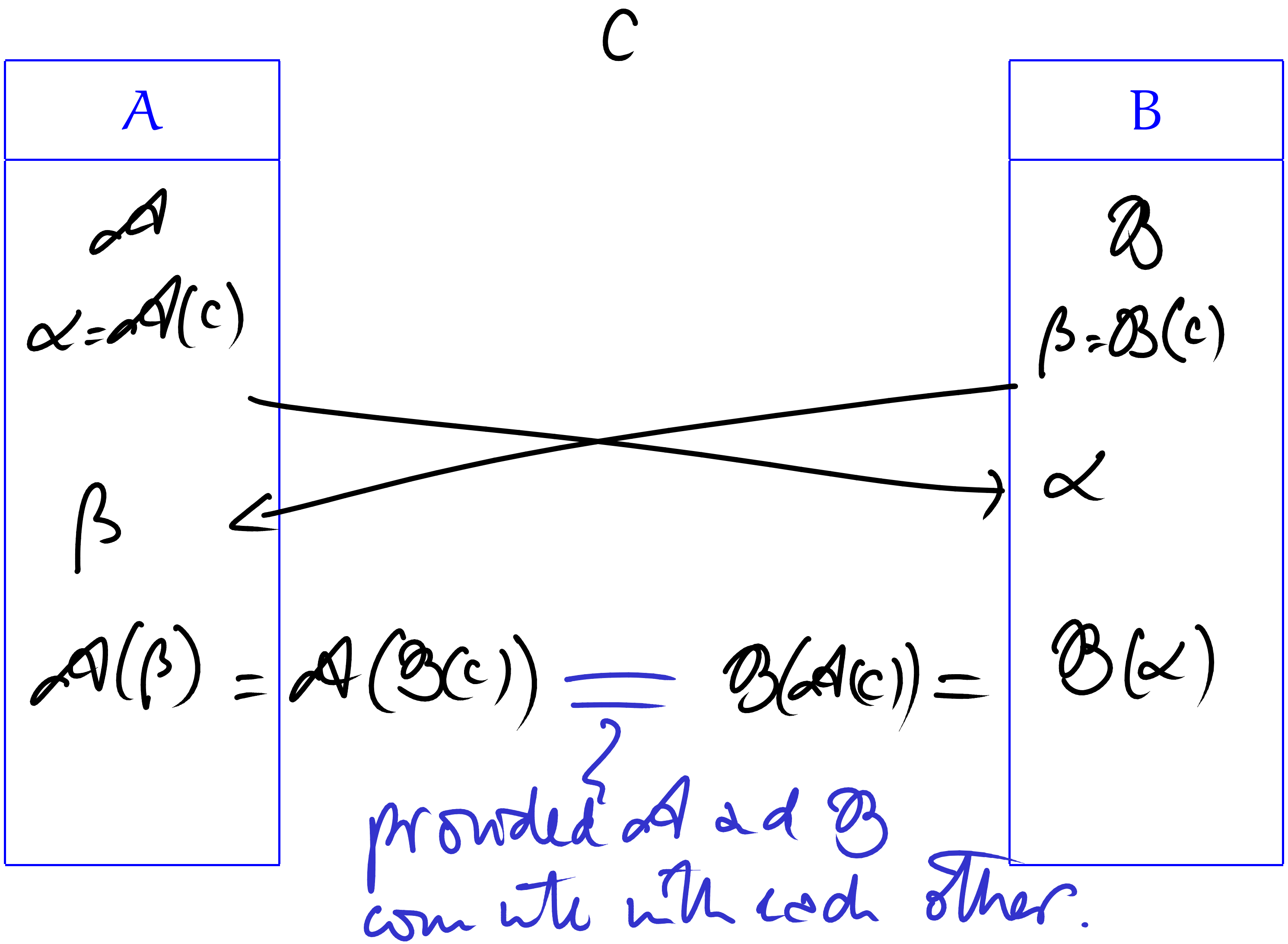
2. *whenever* $\gcd(m,n) = 1$*,*

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

Application to Public-Key Cryptography

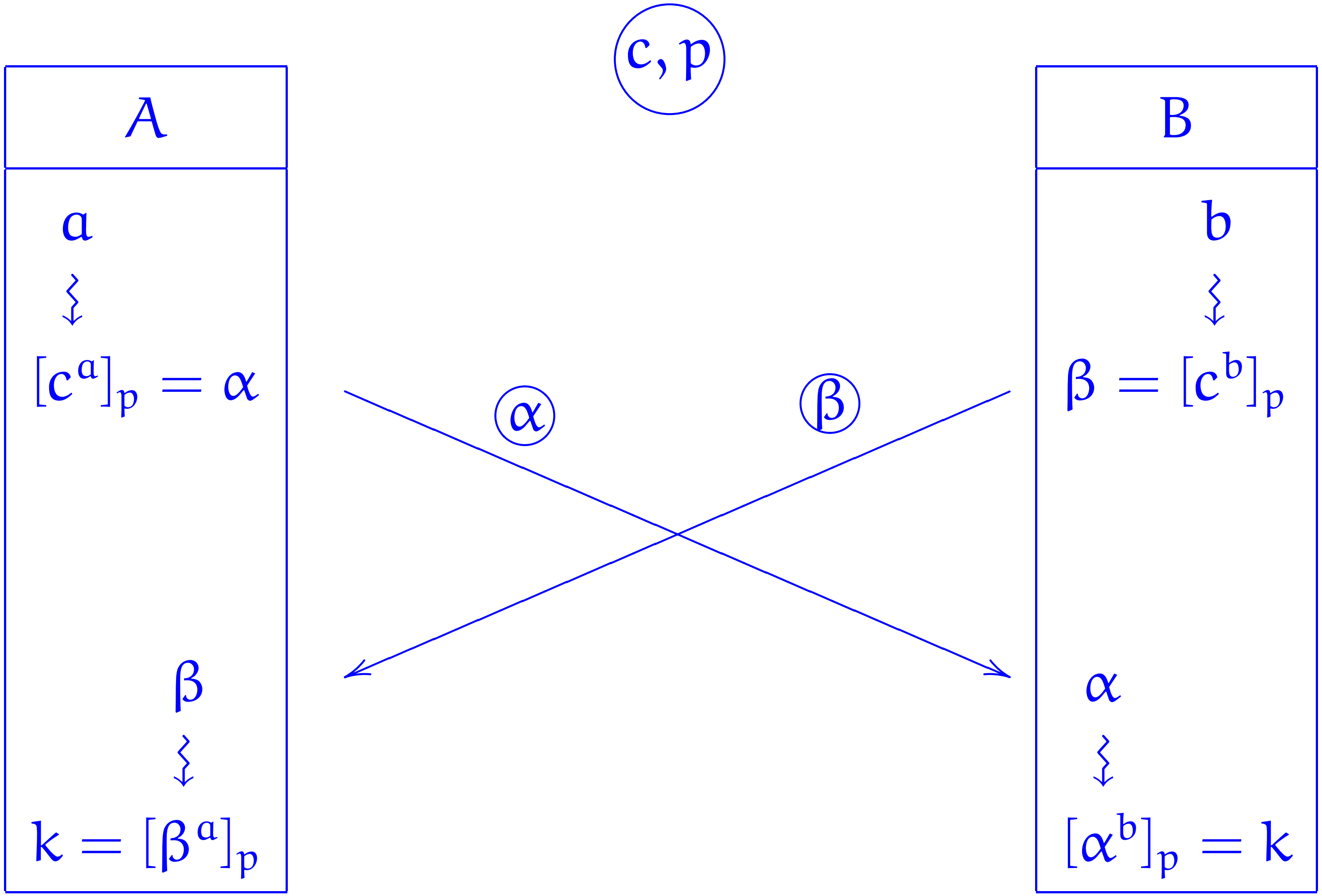
Diffie-Hellman cryptographic method

Shared secret key

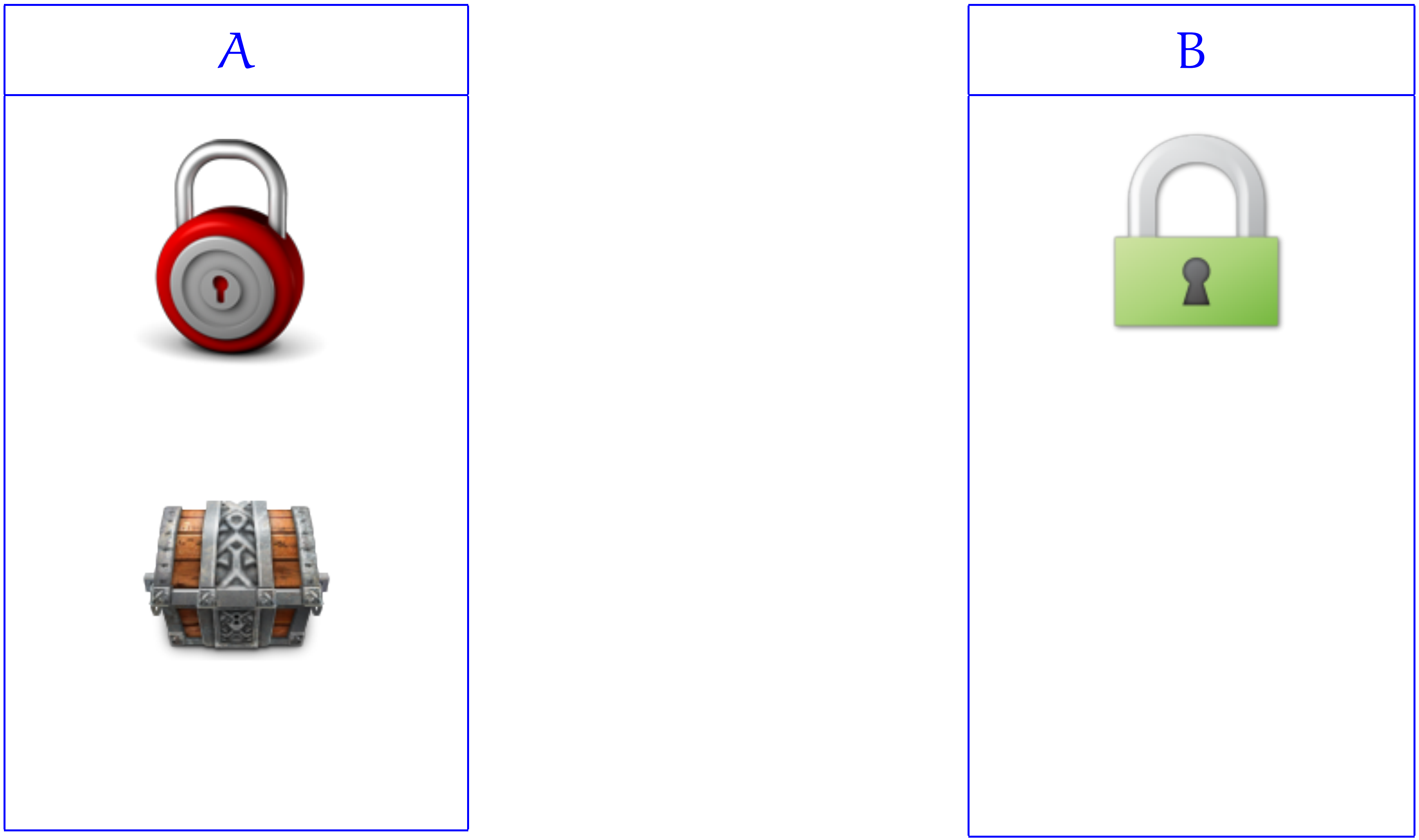


Diffie-Hellman cryptographic method

Shared secret key



Key exchange



Key exchange

Key exchange

A	B
	 

Key exchange

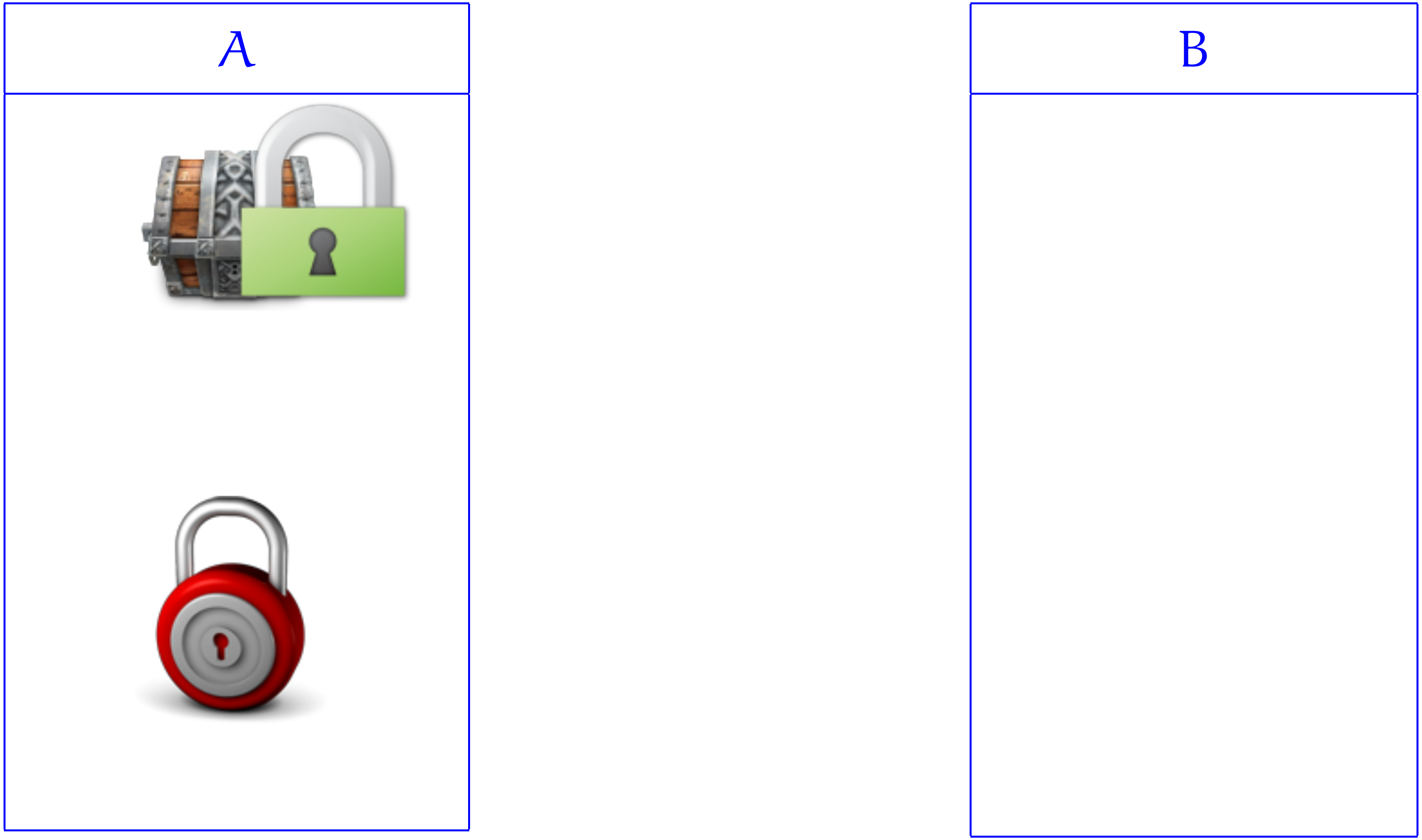
A

B

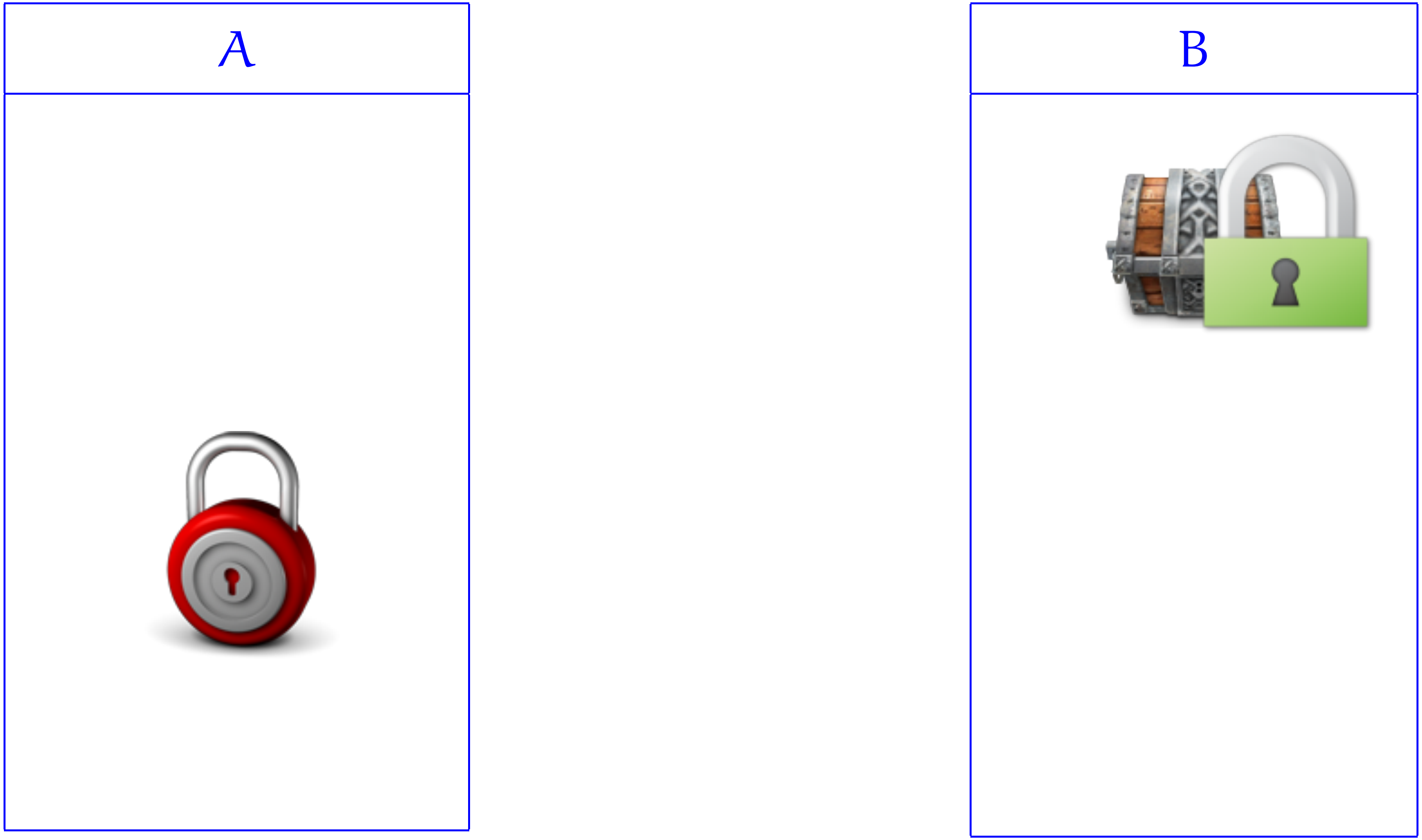
Key exchange

A	B
	

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, $de \equiv 1 \pmod{p}$.

Def Two positive int. m and n are said to be coprime or relative prime whenever $\gcd(m,n)=1$.

Key exchange

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

$$d = \left[\, lc_2(p-1, e) \,\right]_{p-1} \quad .$$

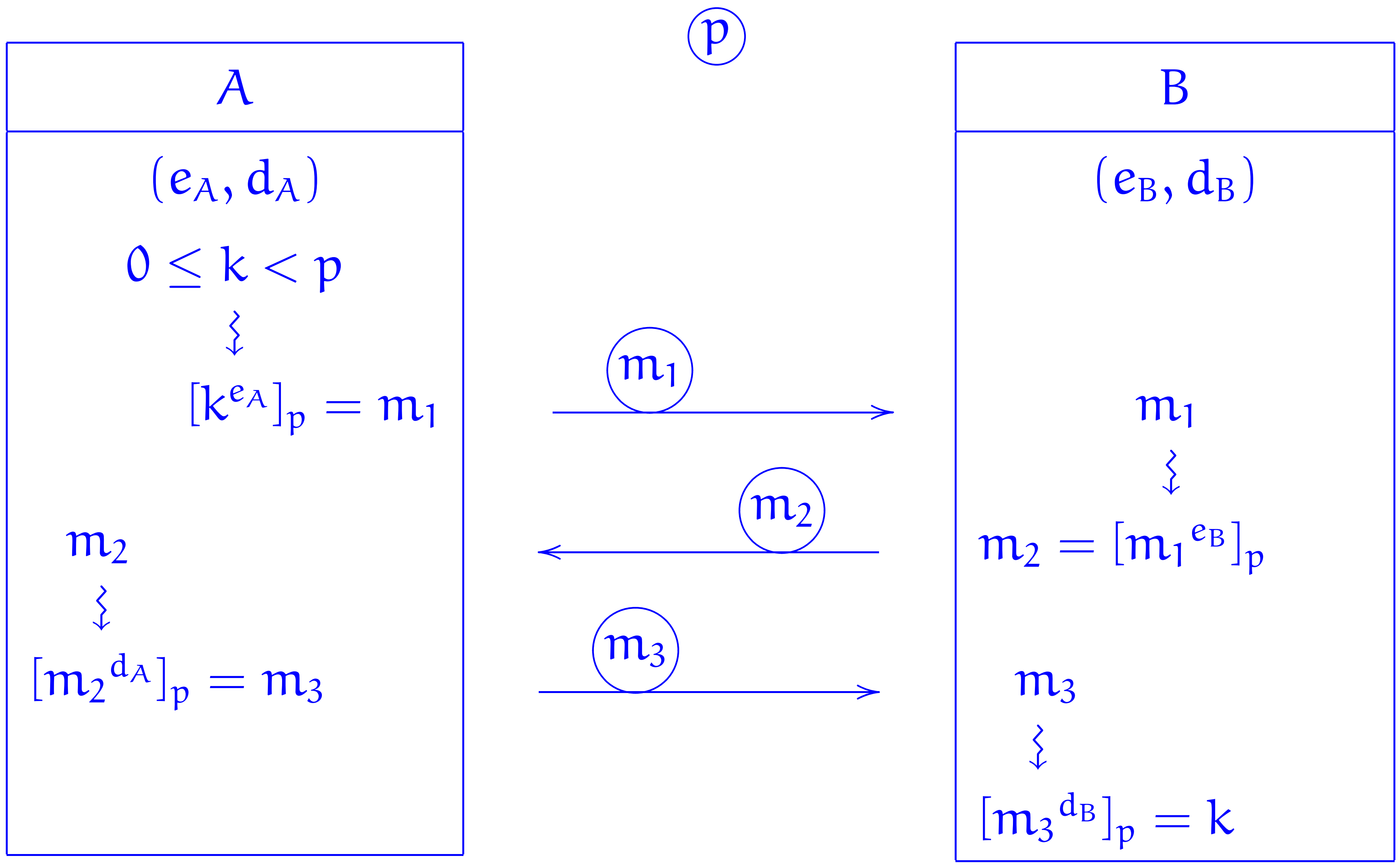
Then, for all integers k,

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

PROOF: We have that $e \cdot d + c(p-1) = 1$ for some int. c in fact negative.

$$k^{ed} = k^{1-c(p-1)} \equiv k \pmod{p} \text{ by FLT.}$$

⊠


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
$m_2 = [m_1{}^{e_B}]_p$
m_2
m_2
$[m_2{}^{d_A}]_p = m_3$
m_3
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 $(k^e)^d \equiv k \pmod{p \cdot q}$

$\boxtimes$