

Discrete Algebraic Structures

WiSe 2025/2026

Prof. Dr. Antoine Wiehe
Research Group for Theoretical Computer Science



Definition. Let $d \geq 2$. Define $a \equiv_d b$ by “ b and b' have the same remainder in the division by d ”
We then say that a and b are **congruent modulo d** .

Equivalence relation with d equivalence classes Set of equivalence classes: $\mathbb{Z}/d\mathbb{Z}$

Definition. Let $d \geq 2$. Define $a \equiv_d b$ by “ b and b' have the same remainder in the division by d ”
We then say that a and b are **congruent modulo d** .

Equivalence relation with d equivalence classes Set of equivalence classes: $\mathbb{Z}/d\mathbb{Z}$

Definition. We **define** addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ as follows:

- $[a]_d + [b]_d$ is defined to be $[a + b]_d$
- $[a]_d \times [b]_d$ is defined to be $[a \times b]_d$

+	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$			
$[1]_3$			
$[2]_3$			

\times	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$			
$[1]_3$			
$[2]_3$			

Definition. Let $d \geq 2$. Define $a \equiv_d b$ by “ b and b' have the same remainder in the division by d ”
We then say that a and b are **congruent modulo d** .

Equivalence relation with d equivalence classes Set of equivalence classes: $\mathbb{Z}/d\mathbb{Z}$

Definition. We **define** addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ as follows:

- $[a]_d + [b]_d$ is defined to be $[a + b]_d$
- $[a]_d \times [b]_d$ is defined to be $[a \times b]_d$

+	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

\times	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

Definition. Let $a \in \mathbb{Z}$. An **inverse** of a modulo d is a number $b \in \mathbb{Z}$ such that $a \times b \equiv_d 1$.

Theorem. Let $a \in \mathbb{Z}$ and $d \geq 2$. Then a has an inverse modulo d if, and only if, a and d are **coprime**.

Definition. Let $n \geq 1$. Define $\varphi(n)$ to be the **number** of numbers in $\{0, \dots, n-1\}$ that have an inverse modulo n .

$$\varphi(n) = |\{a \in \{0, \dots, n-1\} \mid \gcd(a, n) = 1\}|$$

Definition. Let $n \geq 1$. Define $\varphi(n)$ to be the **number** of numbers in $\{0, \dots, n - 1\}$ that have an inverse modulo n .

$$\varphi(n) = |\{a \in \{0, \dots, n - 1\} \mid \gcd(a, n) = 1\}|$$

n	1	2	3	4	5	6	7	8	9
	{0}	{1}	{1, 2}	{1, 3}	{1, 2, 3, 4}	{1, 5}	{1, 2, 3, 4, 5, 6}	{1, 3, 5, 7}	{1, 2, 4, 5, 7, 8}
$\varphi(n)$	1	1	2	2	4	2	6	4	6

Theorem. Let n have prime decomposition $p_1^{e_1} \times \dots \times p_k^{e_k}$.
Then $\varphi(n) = \prod_{i=1}^k (p_i - 1)p_i^{e_i-1}$.

Theorem (Fermat's little theorem). If a and n are **coprime**, then $a^{\varphi(n)} = 1 \bmod n$.

Theorem. Let m, n be **coprime**. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \dots, mn - 1\}$.

Theorem. Let m, n be **coprime**. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \dots, mn - 1\}$.

Proof of existence:

Proof of uniqueness:

Theorem. Let m, n be **coprime**. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \dots, mn - 1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n :

$$um + vn = 1$$

Proof of uniqueness:

Theorem. Let m, n be **coprime**. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \dots, mn - 1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n :

$$um + vn = 1$$

- Define $x = umb + vna$

Proof of uniqueness:

Theorem. Let m, n be **coprime**. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \dots, mn - 1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n :

$$um + vn = 1$$

- Define $x = umb + vna$
- Divide x by mn with remainder to get a solution in $\{0, \dots, mn - 1\}$

Proof of uniqueness:

Theorem. Let m, n be **coprime**. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \dots, mn - 1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n :

$$um + vn = 1$$

- Define $x = umb + vna$
- Divide x by mn with remainder to get a solution in $\{0, \dots, mn - 1\}$

Proof of uniqueness:

- Define $f: \{0, \dots, mn - 1\} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $f(x) = ([x]_m, [x]_n)$

Theorem. Let m, n be **coprime**. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \dots, mn - 1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n :

$$um + vn = 1$$

- Define $x = umb + vna$
- Divide x by mn with remainder to get a solution in $\{0, \dots, mn - 1\}$

Proof of uniqueness:

- Define $f: \{0, \dots, mn - 1\} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $f(x) = ([x]_m, [x]_n)$
- We proved that f is...

Theorem. Let m, n be **coprime**. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \dots, mn - 1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n :

$$um + vn = 1$$

- Define $x = umb + vna$
- Divide x by mn with remainder to get a solution in $\{0, \dots, mn - 1\}$

Proof of uniqueness:

- Define $f: \{0, \dots, mn - 1\} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $f(x) = ([x]_m, [x]_n)$
- We proved that f is... **surjective**
- Since the domain and codomain have same size, f must be **injective**!

Theorem. Let m, n be **coprime**. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \dots, mn - 1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n :

$$um + vn = 1$$

- Define $x = umb + vna$
- Divide x by mn with remainder to get a solution in $\{0, \dots, mn - 1\}$

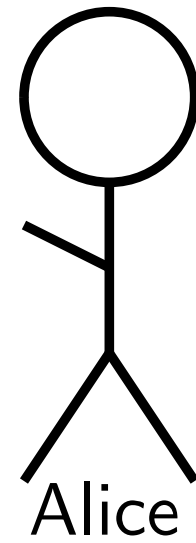
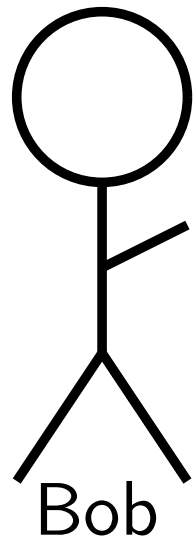
Proof of uniqueness:

- Define $f: \{0, \dots, mn - 1\} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $f(x) = ([x]_m, [x]_n)$
- We proved that f is... **surjective**
- Since the domain and codomain have same size, f must be **injective**!
- This means
if $[x]_m = [y]_m$ and $[x]_n = [y]_n$, then $x = y$.

Symmetric Cryptography

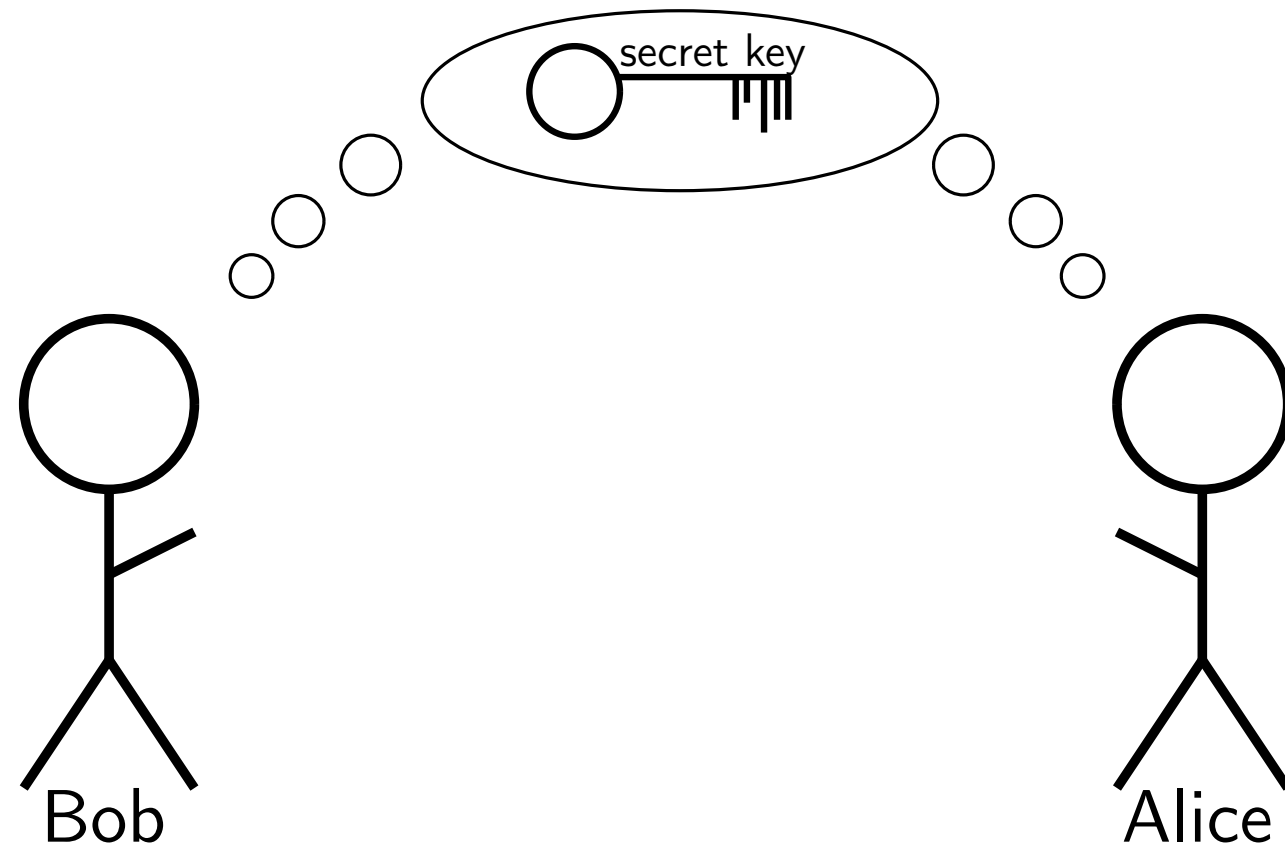
Asymmetric Cryptography

Symmetric Cryptography



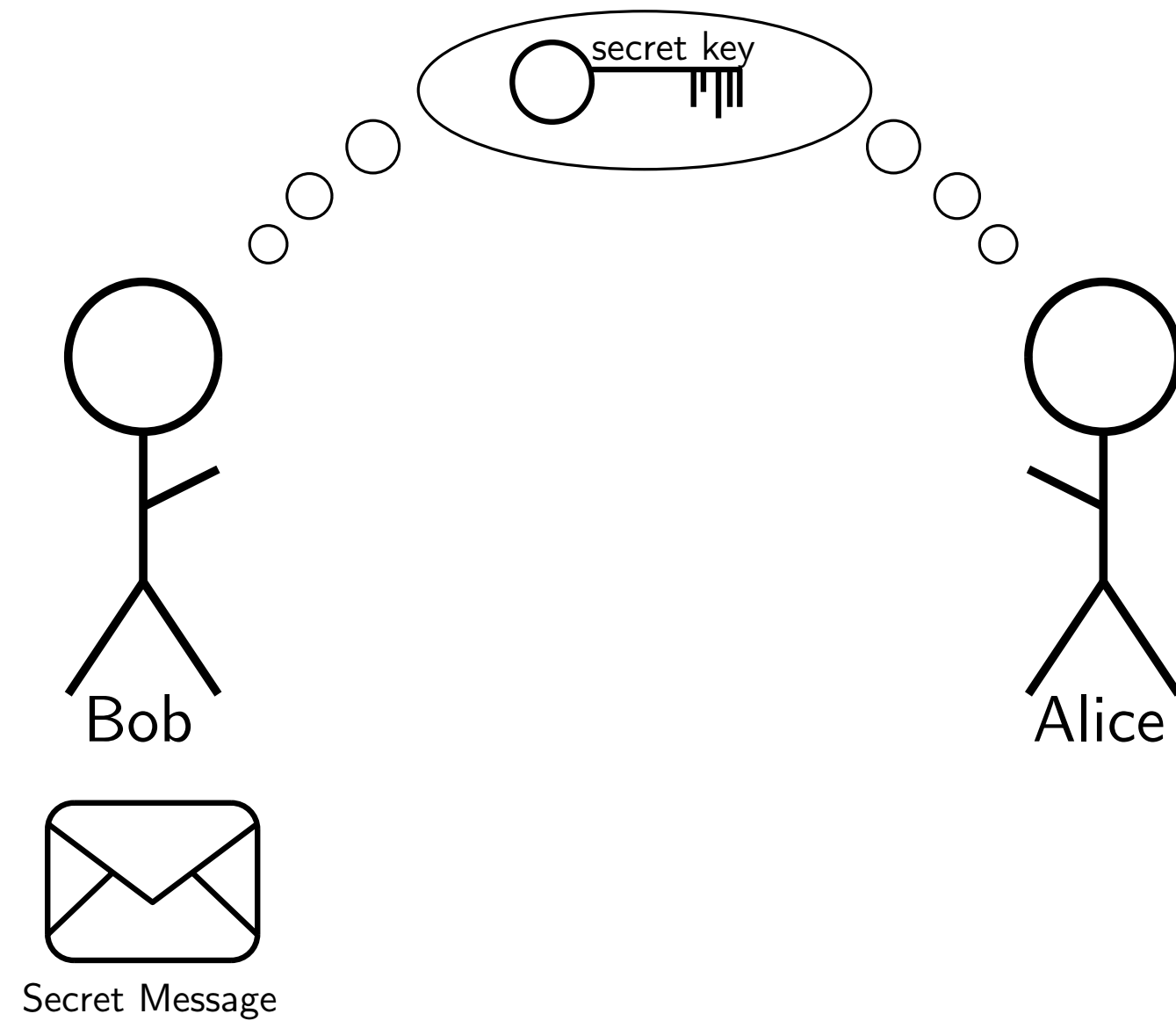
Asymmetric Cryptography

Symmetric Cryptography



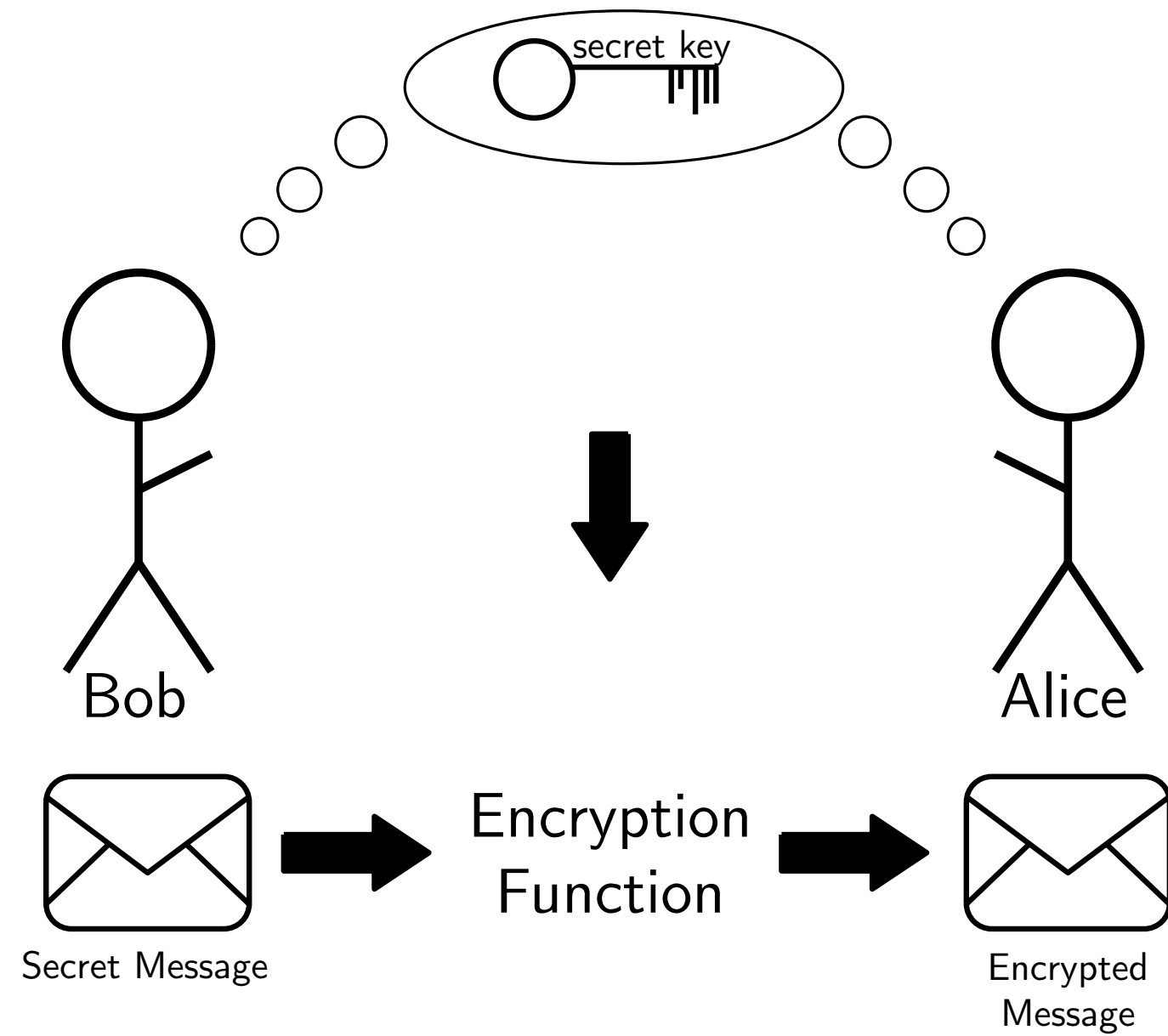
Asymmetric Cryptography

Symmetric Cryptography



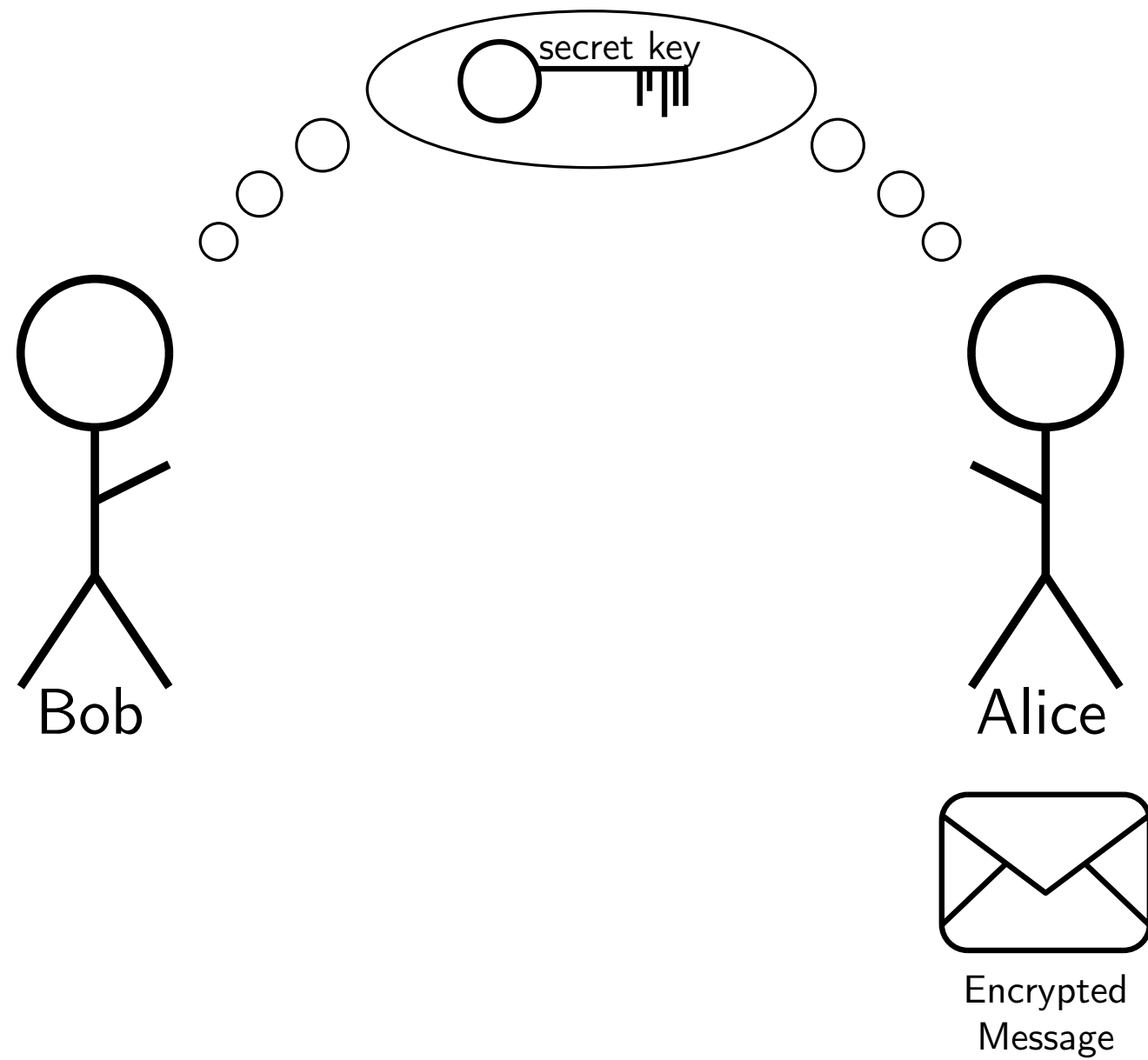
Asymmetric Cryptography

Symmetric Cryptography



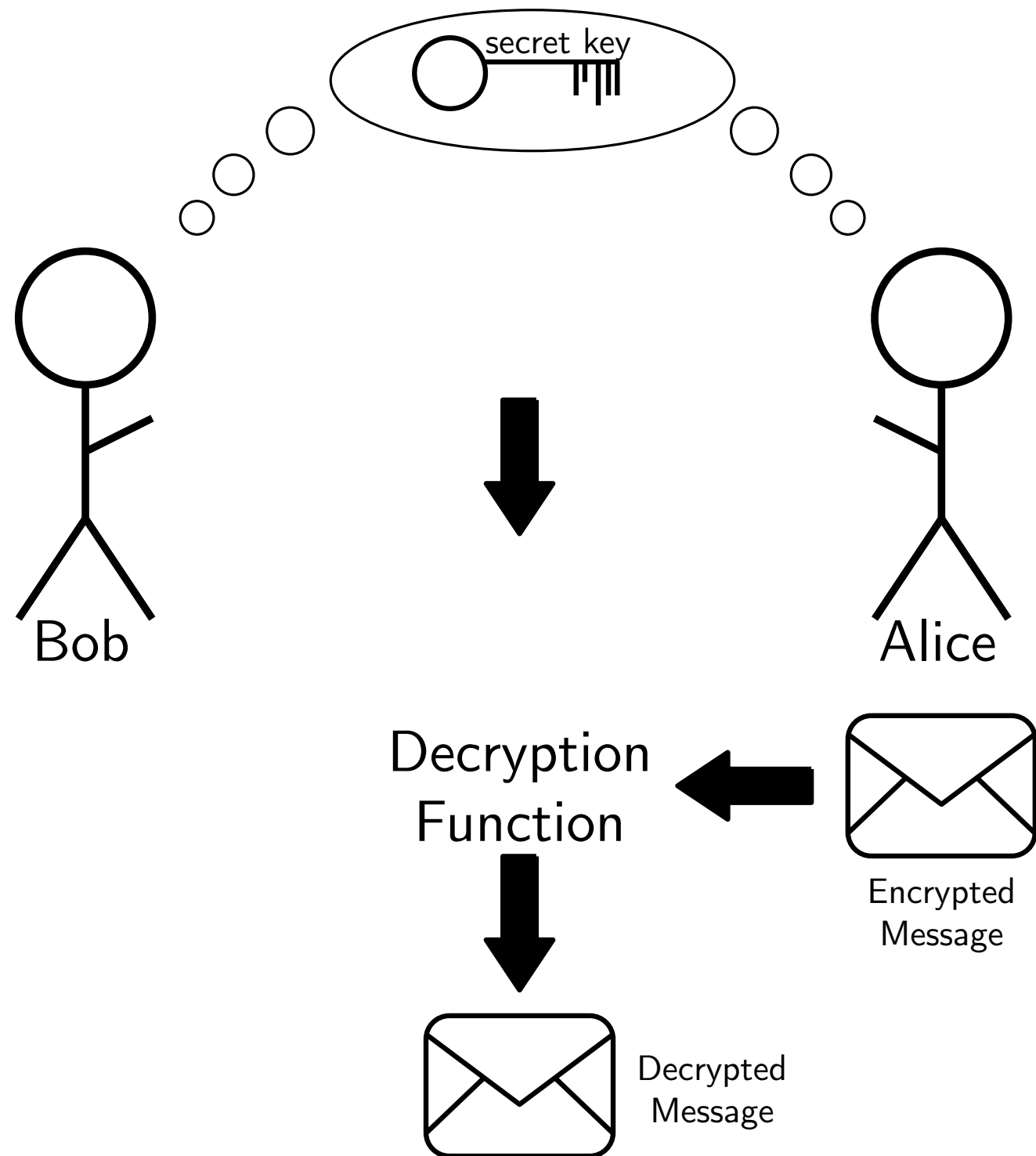
Asymmetric Cryptography

Symmetric Cryptography



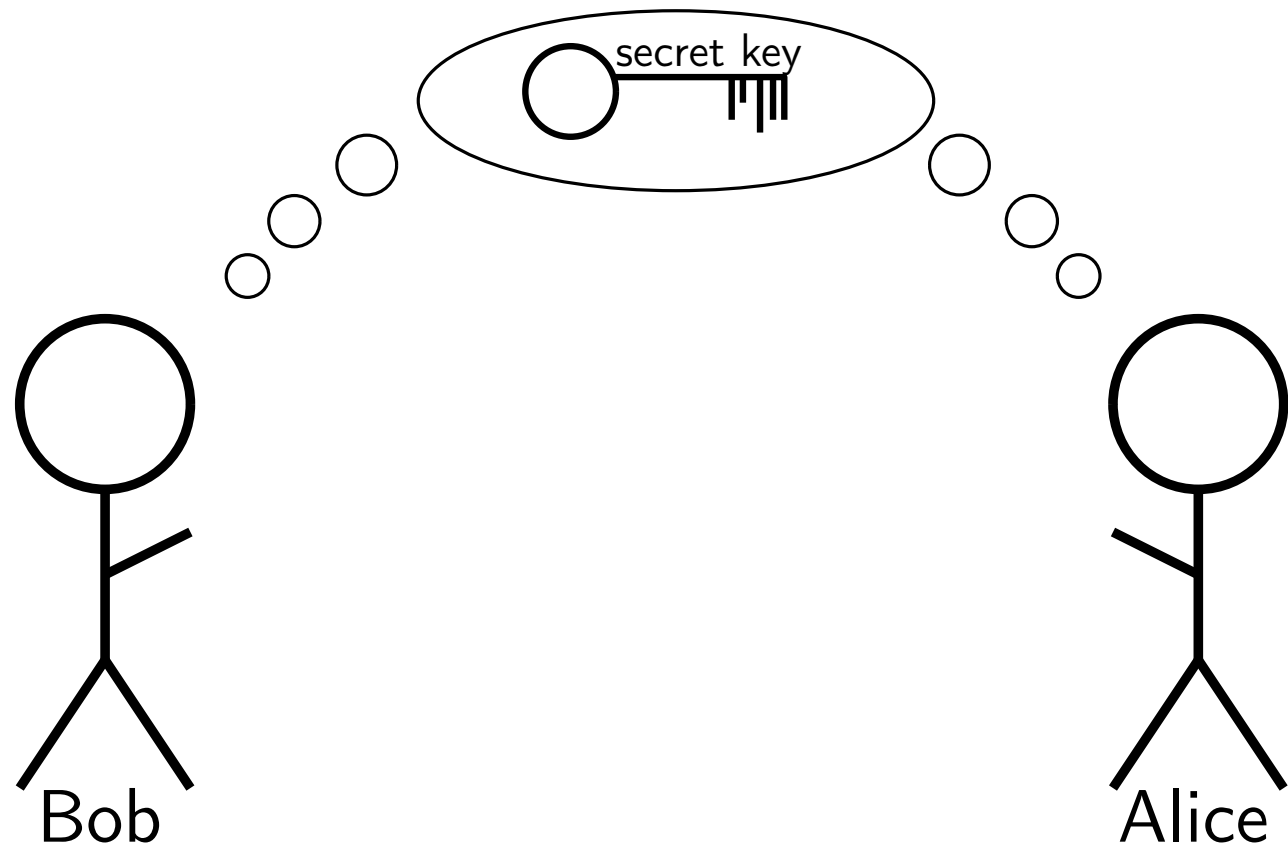
Asymmetric Cryptography

Symmetric Cryptography

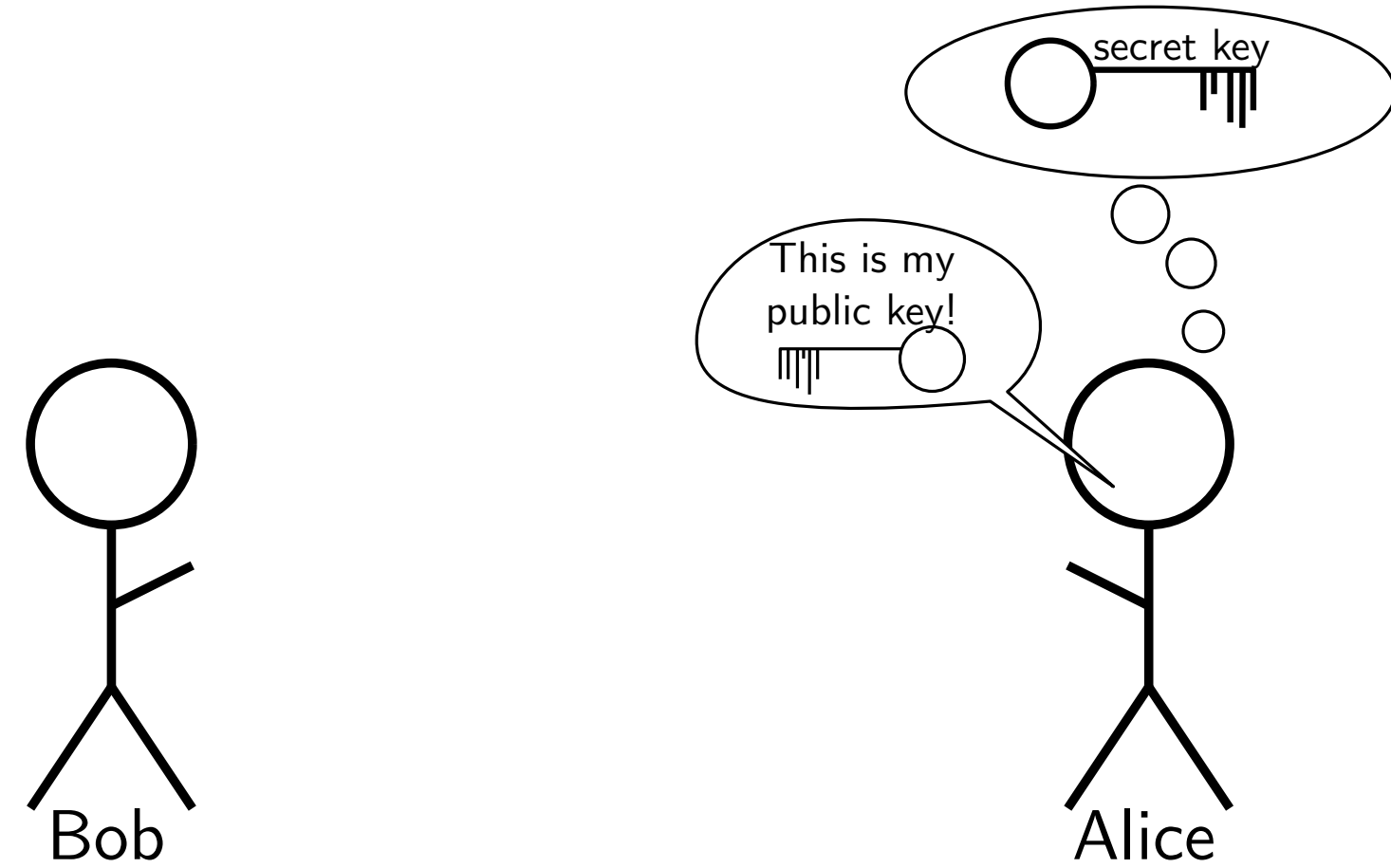


Asymmetric Cryptography

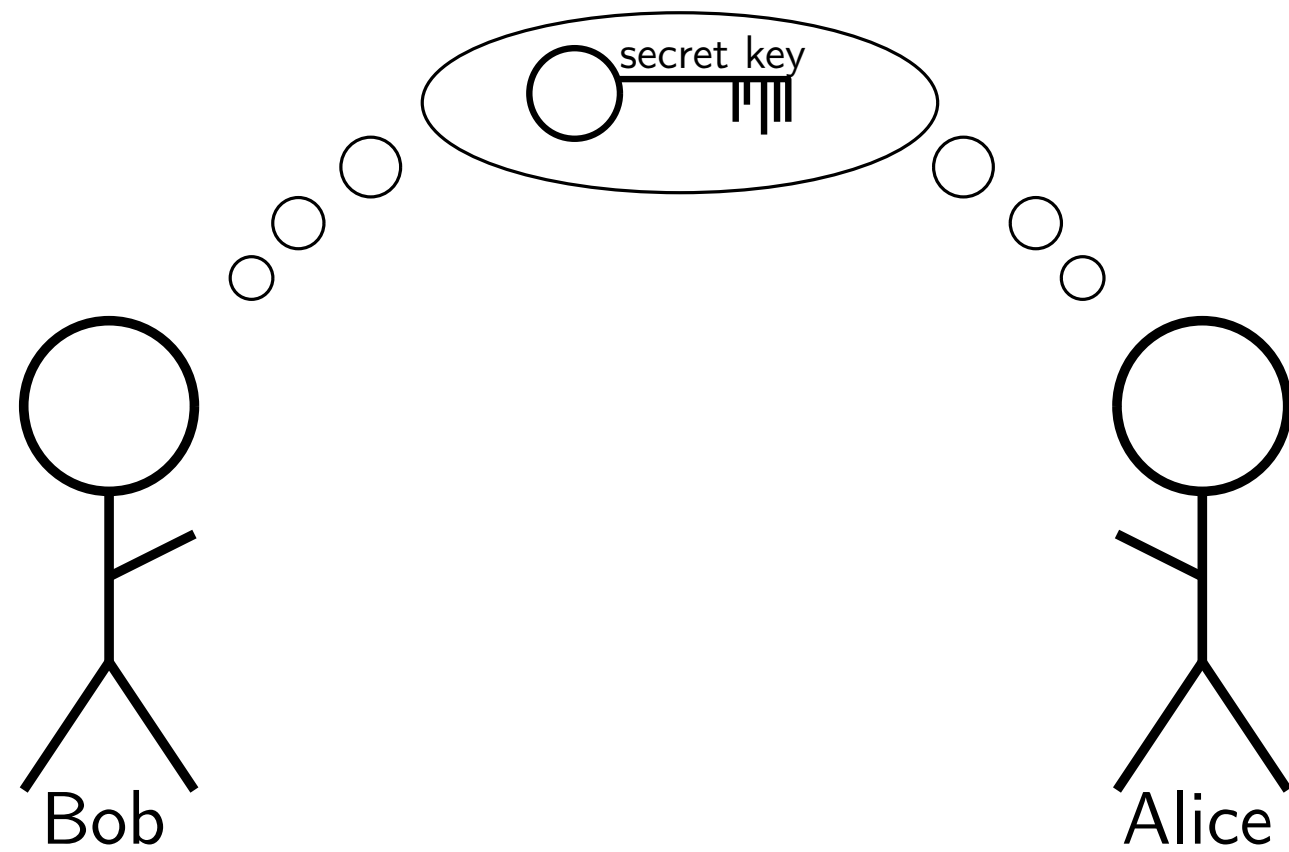
Symmetric Cryptography



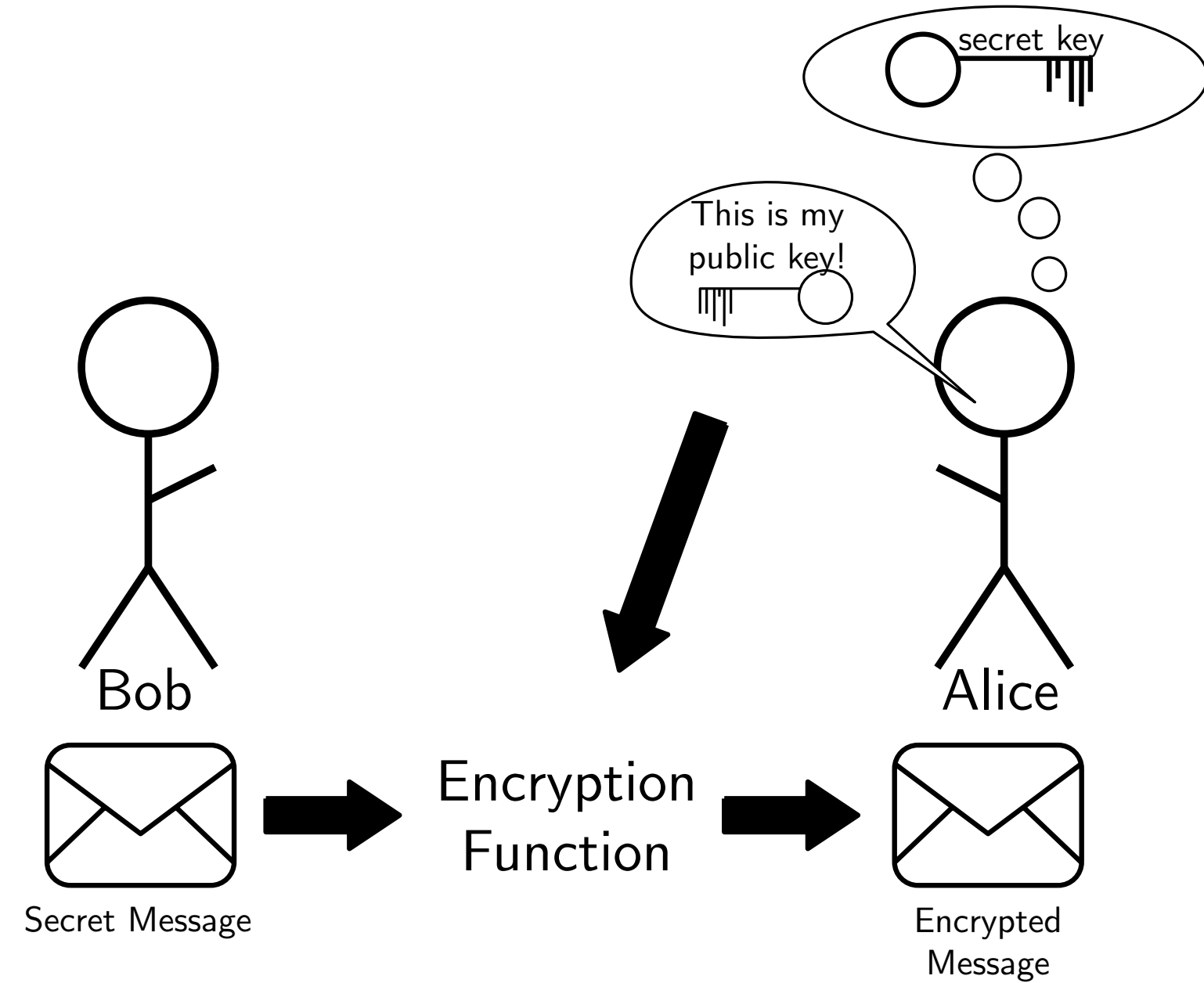
Asymmetric Cryptography



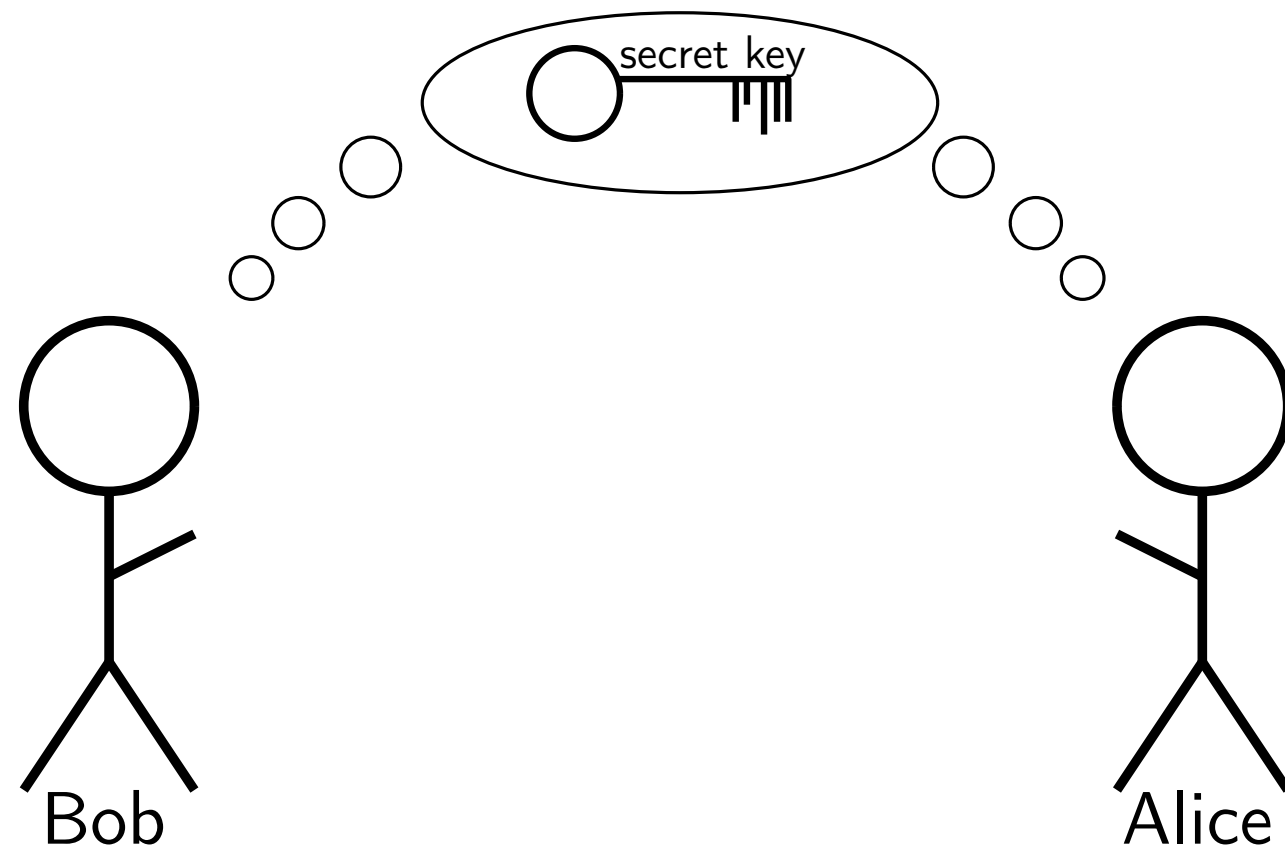
Symmetric Cryptography



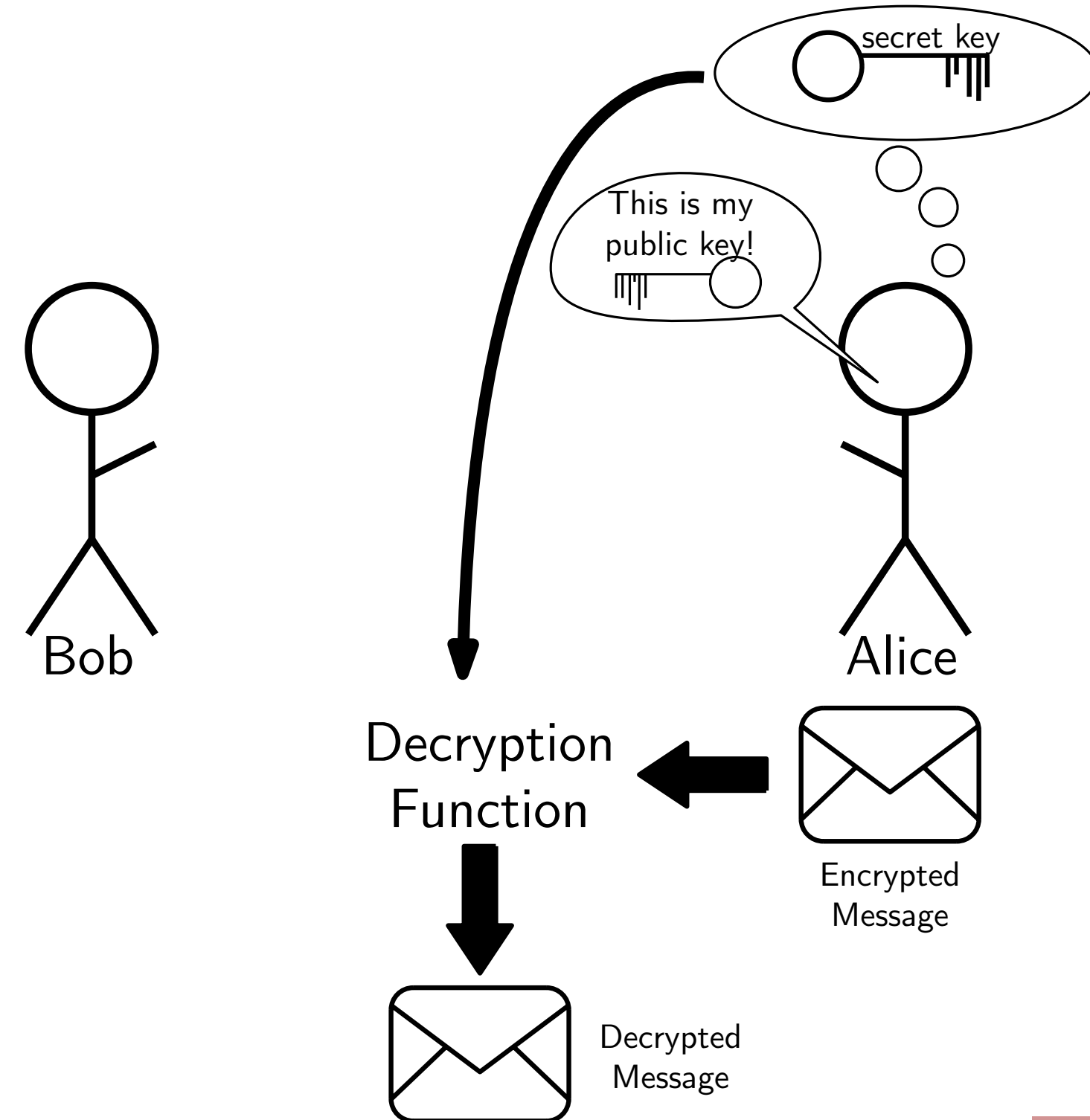
Asymmetric Cryptography



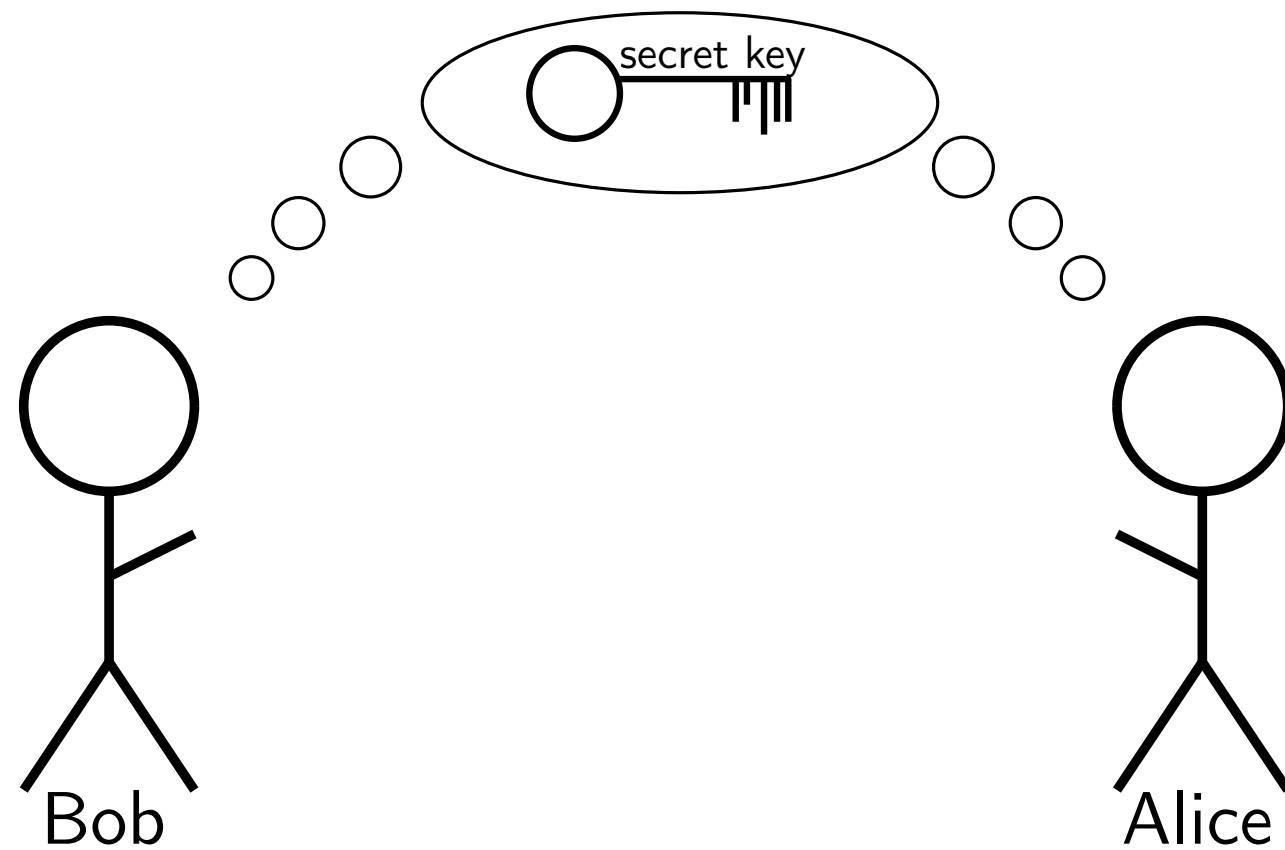
Symmetric Cryptography



Asymmetric Cryptography



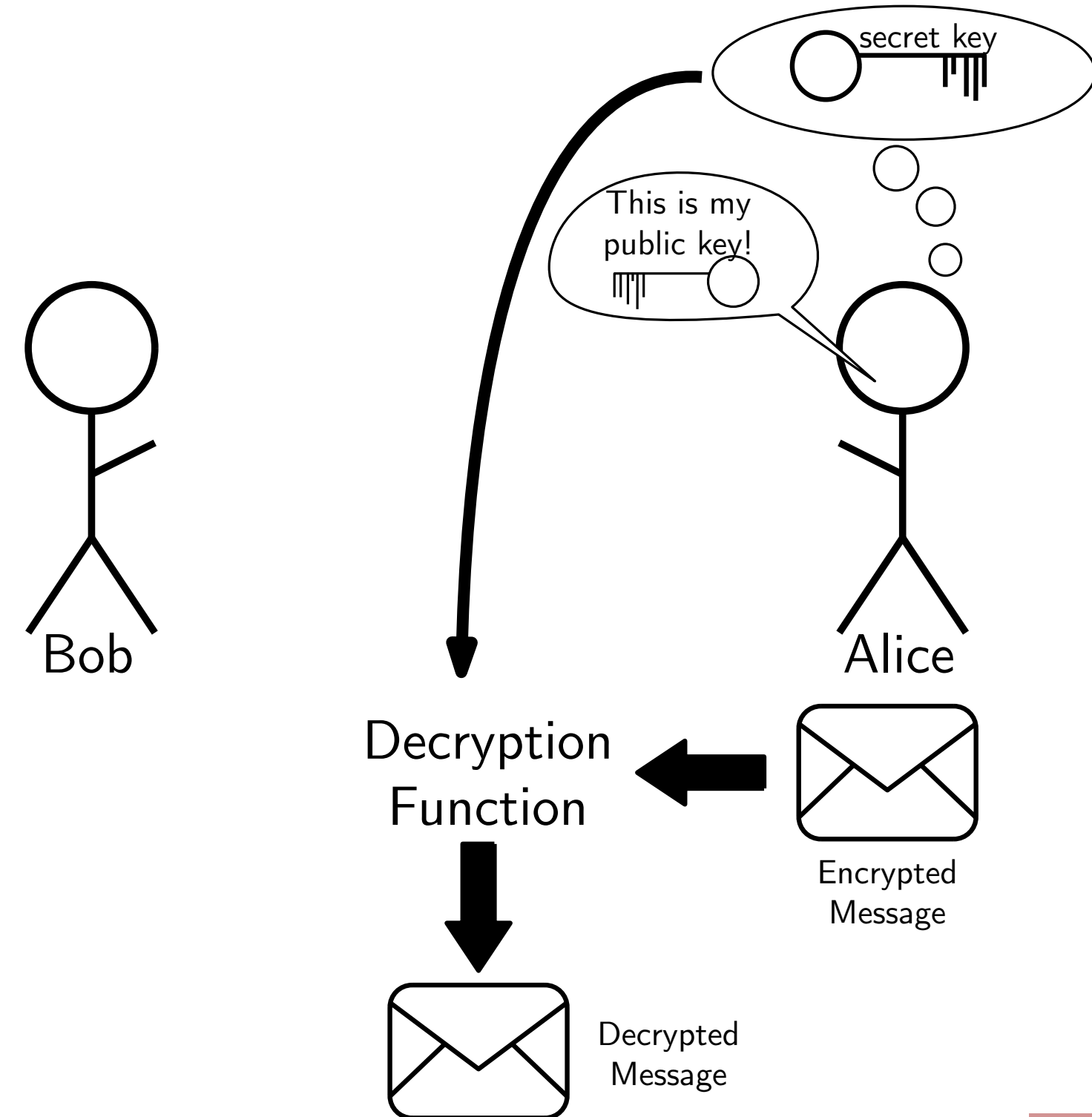
Symmetric Cryptography



Advantages compared to symmetric crypto:

- If n people want to write Alice, no need for Alice to create n different keys
- Can also be used to **sign** messages

Asymmetric Cryptography



- Keys and messages are (tuples of) **numbers**
- Messages can be seen as elements of $\mathbb{Z}/n\mathbb{Z}$
- Example of RSA key:
~/.ssh/id_rsa.pub

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGD6LhW7+bdi195HW/D3SHMUX7F8KZrgtfyns+o1hRBRJPmrbvy8ZQu/  
LkZE8iNGP4Ti7gYXom4XyC3DkSmtafm+nofy73lnvFlG5QvQxtfaBHT15IHhNXxiFHo6wt+MCVIMFu/JFtxOmQJSn8NB  
F46zfYMgKVWEiTNPk2f4HERVvKNh41gB2JNzaxDg8TEh1ft4t2HpL8eLhzpxvUjusBw+2hz7bfzGVsgrIVYcw9MBcTR  
aRFRcZMnXaUe7BiySHTKLCS1Ysc1UXrdLg8qGSMHH2vT1gUY/VQ3EF5nmHku+4Cv894wpQbyGJ02fK1e/Vd/pbI43lDX  
tiEa7o4uE9oKGpp6tbq6AH1HzVHjFAnYk5sBoEFg4fd+VEaxn5BIH3A19mpsbfa00064DqyHsX4D8nkvh1wo7cpvW3ex  
HBq/3bxFW6HKPn72Qe0xLevDfDe2tekiBtwVesiKs92S1xh2Z484FbriBPtdsFF1pyk/y9ya1vjqt4fxI8aNqrcqfyM=
```

Number in **base 64**

- Keys and messages are (tuples of) **numbers**
- Messages can be seen as elements of $\mathbb{Z}/n\mathbb{Z}$
- Example of RSA key:
~/.ssh/id_rsa.pub

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGD6LhW7+bdi195HW/D3SHMUX7F8KZrgtfyns+o1hRBRJPmrbvy8ZQu/  
LkZE8iNGP4Ti7gYXom4XyC3DkSmtafm+nofy73lnvFlG5QvQxtfaBHT15IHhNXxiFHo6wt+MCVIMFu/JFtxOmQJSn8NB  
F46zfYMgKVWEiTNPk2f4HERVKNh41gB2JNzaxDg8TEh1ft4t2HpL8eLhzpxvUjusBw+2hz7bfzGVSgrIVYcw9MBcTR  
aRFRcZMnXaUe7BiySHTKLCS1Ysc1UXrdLg8qGSMHH2vT1gUY/VQ3EF5nmHku+4Cv894wpQbyGJ02fK1e/Vd/pbI43lDX  
tiEa7o4uE9oKGpp6tbq6AH1HzVHjFAnYk5sBoEFg4fd+VEaxn5BIH3A19mpsbfa00064DqyHsX4D8nkvh1wo7cpvW3ex  
HBq/3bxFW6HKPn72Qe0xLevDfDe2tekiBtwVesiKs92S1xh2Z484FbriBPtdsFF1pyk/y9ya1vjqt4fxI8aNqrcqfyM=
```

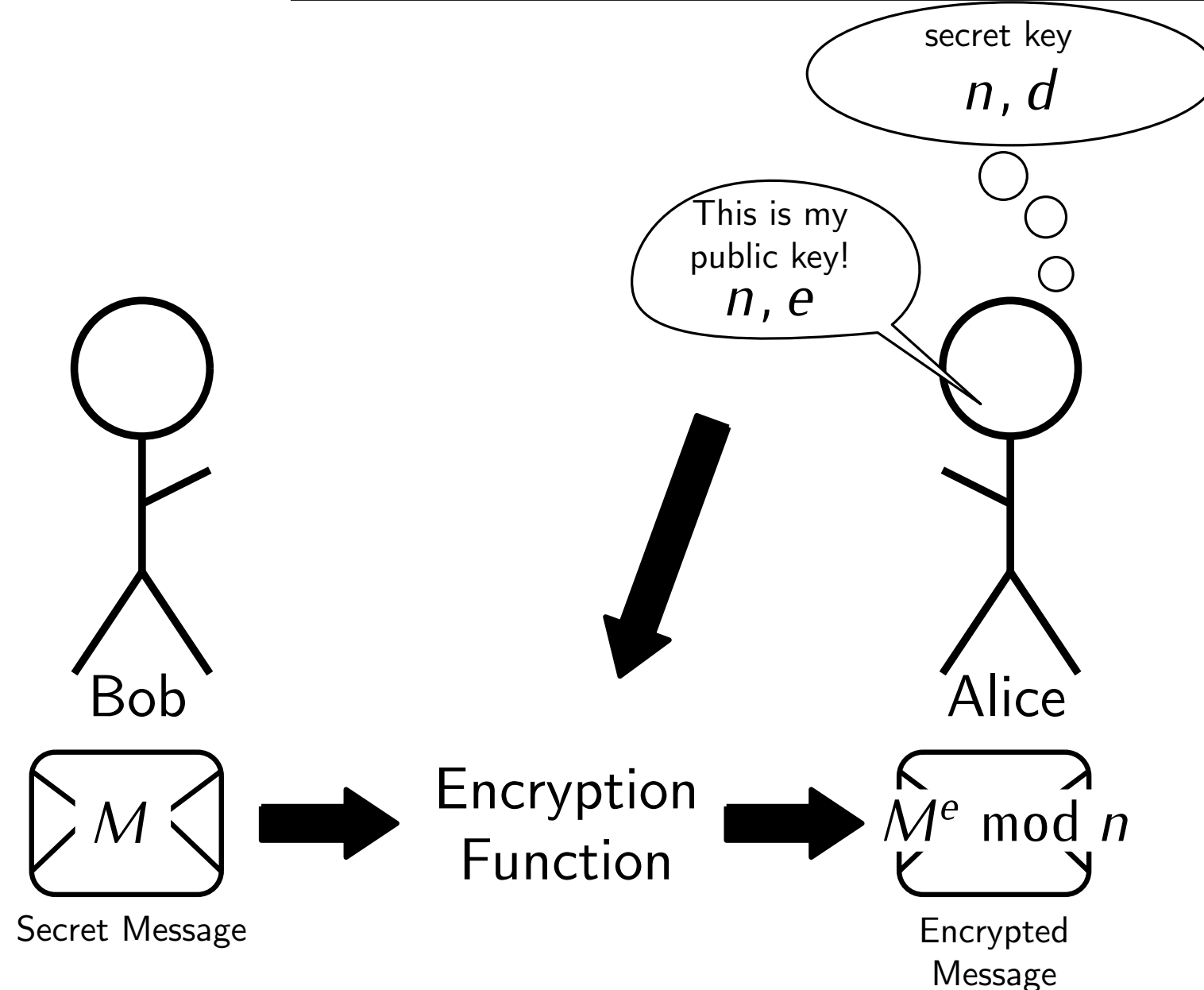
Number in **base 64**

n = 5677528668400117464635445009368862501114000657308498941562452977981671248196334
53907235687927854028945433075256023603482475622628050511765625505980788742387062054
42114668909534038111800378549288212990518723891664097295909644118933886302215135183
08281597872349593351801124144562894949756365032222936258311012340879184966986244896
27407986048217152067805164292793251529563302630003531744019209469508394783908243723
80501044511072359577346288143786635609460155282889733084407153794255465828374819589
77510114945361636157975815374571286570294638015146473013296495239941766655054219332
27765799135681549359968831573569986337714436450544812478862975125067800964594296674
38203895575921349105248292764852707602678812527328330439546283242613427790901489073
13301774882173450123517095906335038959343975914227747264843122062037932620153140218
39217793300991829666712747175627185177612969282716497065323469353415915994982154493
4368212685586211 and **e** = 17

- Keys and messages are (tuples of) **numbers**
- Messages can be seen as elements of $\mathbb{Z}/n\mathbb{Z}$
- Example of RSA key:
~/.ssh/id_rsa.pub

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGD6LhW7+bdi195HW/D3SHMUX7F8KZrgtfyns+o1hRBRJPmrbvy8ZQu/
LkZE8iNGP4Ti7gYXom4XyC3DkSmtafm+nofy73lnvFlG5QvQxtfaBHT15IHhNXxiFHo6wt+MCVIMFu/JFtxOmQJSn8NB
F46zfYMgKVWEiTNPk2f4HERVKNh41gB2JNzaxDg8TEh1ft4t2HpL8eLhzpxvUjusBw+2hz7bfzGVsgrIVYcw9MBcTR
aRFRcZMnXaUe7BiySHTKLCS1Ysc1UXrdLg8qGSMHH2vT1gUY/VQ3EF5nmHku+4Cv894wpQbyGJ02fK1e/Vd/pbI43lDX
tiEa7o4uE9oKGpp6tbq6AH1HzVHjFAnYk5sBoEFg4fd+VEaxn5BIH3A19mpsbfa00064DqyHsX4D8nkvh1wo7cpvW3ex
HBq/3bxFW6HKPn72Qe0xLevDfDe2tekiBtwVesiKs92S1xh2Z484FbriBPtdsFF1pyk/y9ya1vjqt4fxI8aNqrcqfyM=
```

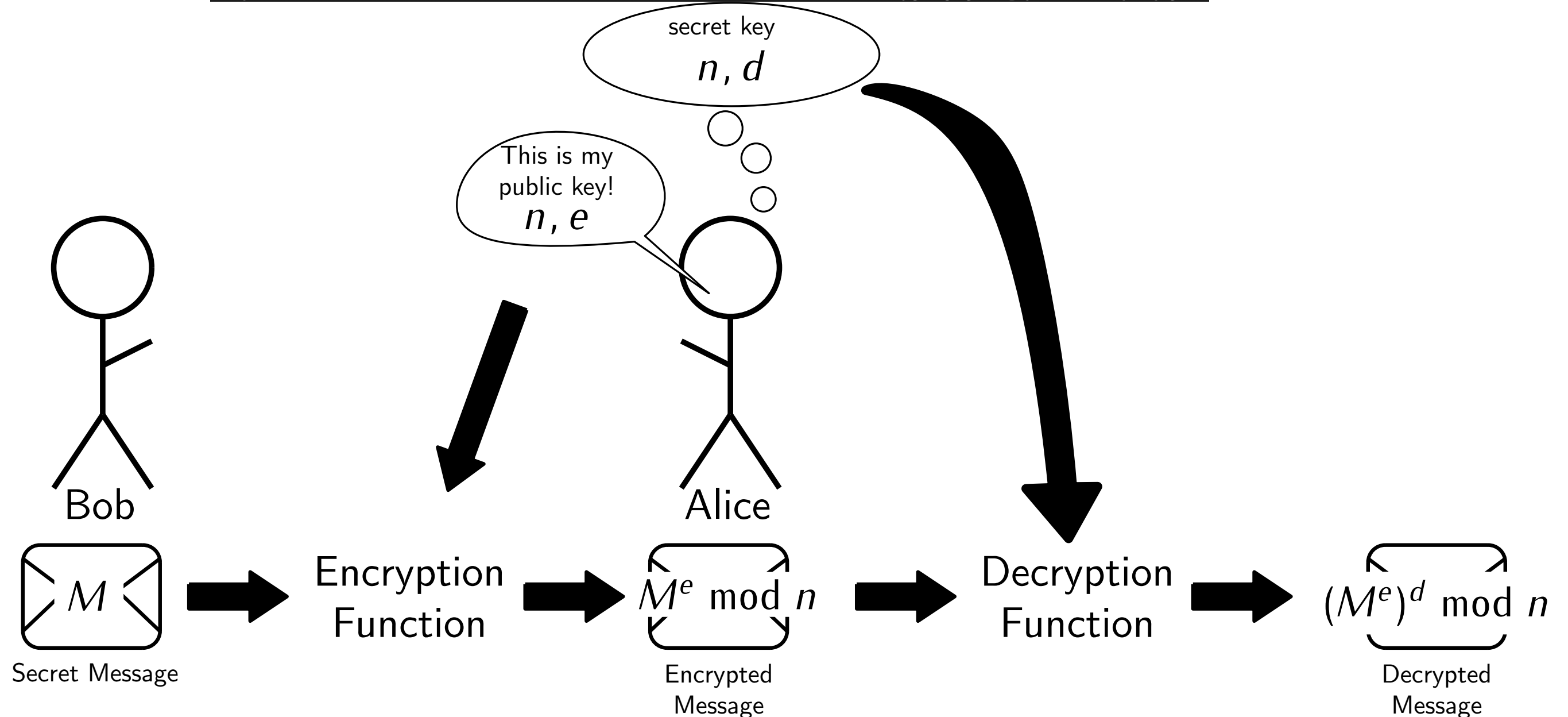
Number in **base 64**



- Keys and messages are (tuples of) **numbers**
- Messages can be seen as elements of $\mathbb{Z}/n\mathbb{Z}$
- Example of RSA key:
~/.ssh/id_rsa.pub

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGD6LhW7+bdi195HW/D3SHMUX7F8KZrgtfyns+o1hRBRJPmrbvy8ZQu/
LkZE8iNGP4Ti7gYXom4XyC3DkSmtafm+nofy73lnvF1G5QvQxtfaBHT15IHhNXxiFHo6wt+MCVIMFu/JFtxOmQJSn8NB
F46zfYMgKVWEiTNPk2f4HERVKNh41gB2JNzaxDg8TEh1ft4t2HpL8eLhzpxvUjusBw+2hz7bfzGVSgrIVYcw9MBcTR
aRFRcZMnXaUe7BiySHTKLCS1Ysc1UXrdLg8qGSMHH2vT1gUY/VQ3EF5nmHku+4Cv894wpQbyGJ02fK1e/Vd/pbI43lDX
tiEa7o4uE9oKGpp6tbq6AH1HzVHjFAnYk5sBoEFg4fd+VEaxn5BIH3A19mpsbfa00064DqyHsX4D8nkvh1wo7cpvW3ex
HBq/3bxFW6HKPn72Qe0xLevDfDe2tekiBtwVesiKs92S1xh2Z484FbriBPtdsFF1pyk/y9ya1vjqt4fxI8aNqrcqfyM=
```

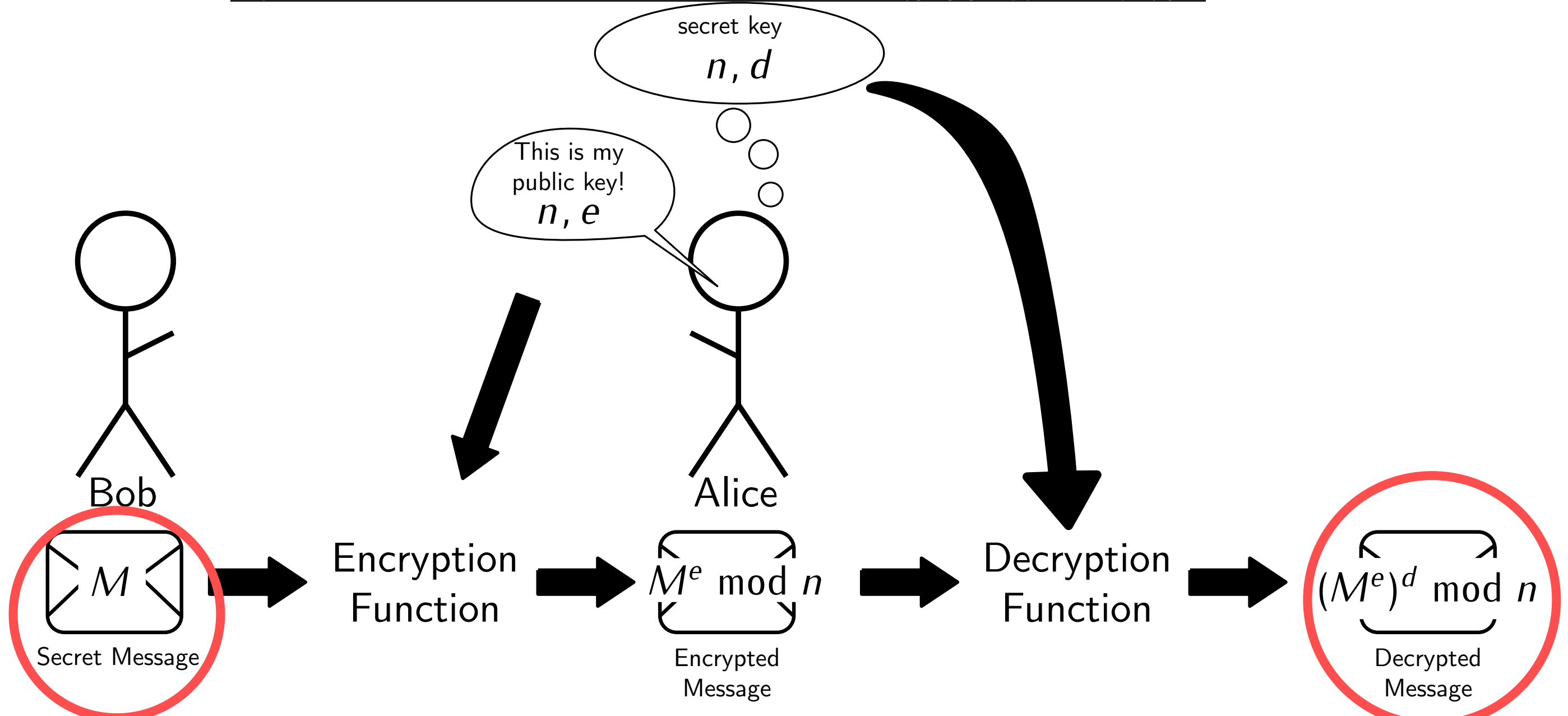
Number in **base 64**



- Keys and messages are (tuples of) **numbers**
- Messages can be seen as elements of $\mathbb{Z}/n\mathbb{Z}$
- Example of RSA key:
~/.ssh/id_rsa.pub

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQD6LhW7+bdi195HW/D3SHMUX7F8KZrgtfyns+o1hRBRJPmrbvy8ZQu/LkZE8iNGP4Ti7gYXom4XyC3DkSmtafm+nofy73lnvF1G5QvQxtfaBHT15IHNNXiFHo6wt+MCVIMFu/JFtxOmQJSn8NB
F46zfYMgKVWEiTNPk2f4HERVKNh41gB2JNzaxDg8TEh1ft4t2HpL8eLhzpxvUjusBw+2hz7bfzGVSgrIVYcw9MBcTR
aRFRcZMnXaUe7BiySHTKLCS1Ysc1UXrdLg8qGSMHH2vT1gUY/VQ3EF5nmHku+4Cv894wpQbyGJ02fK1e/Vd/pbI43lDX
tiEa7o4uE9oKGpp6tbq6AH1HzVHjFAnYk5sBoEFg4fd+VEaxn5BIH3A19mpsbfa00064DqyHsX4D8nkvh1wo7cpvW3ex
HBq/3bxFW6HKPn72Qe0xLevDfDe2tekiBtwVesiKs92S1xh2Z484FbriBPtdsFF1pyk/y9ya1vjqt4fxI8aNqrcqfyM=
```

Number in **base 64**



Want: n, e, d such that $(M^e)^d = M \bmod n$ for all $M \in \mathbb{Z}/n\mathbb{Z}$

Key generation:

- Choose **distinct prime numbers** p and q
- $n := pq$
- $e \in \{2, \dots, \varphi(n) - 1\}$ **coprime** with $\varphi(n)$
- d **inverse** of e modulo $\varphi(n)$

Want: n, e, d such that $(M^e)^d = M \bmod n$ for all $M \in \mathbb{Z}/n\mathbb{Z}$

Key generation:

- Choose **distinct prime numbers** p and q
- $n := pq$
- $e \in \{2, \dots, \varphi(n) - 1\}$ **coprime** with $\varphi(n)$
- d **inverse** of e modulo $\varphi(n)$

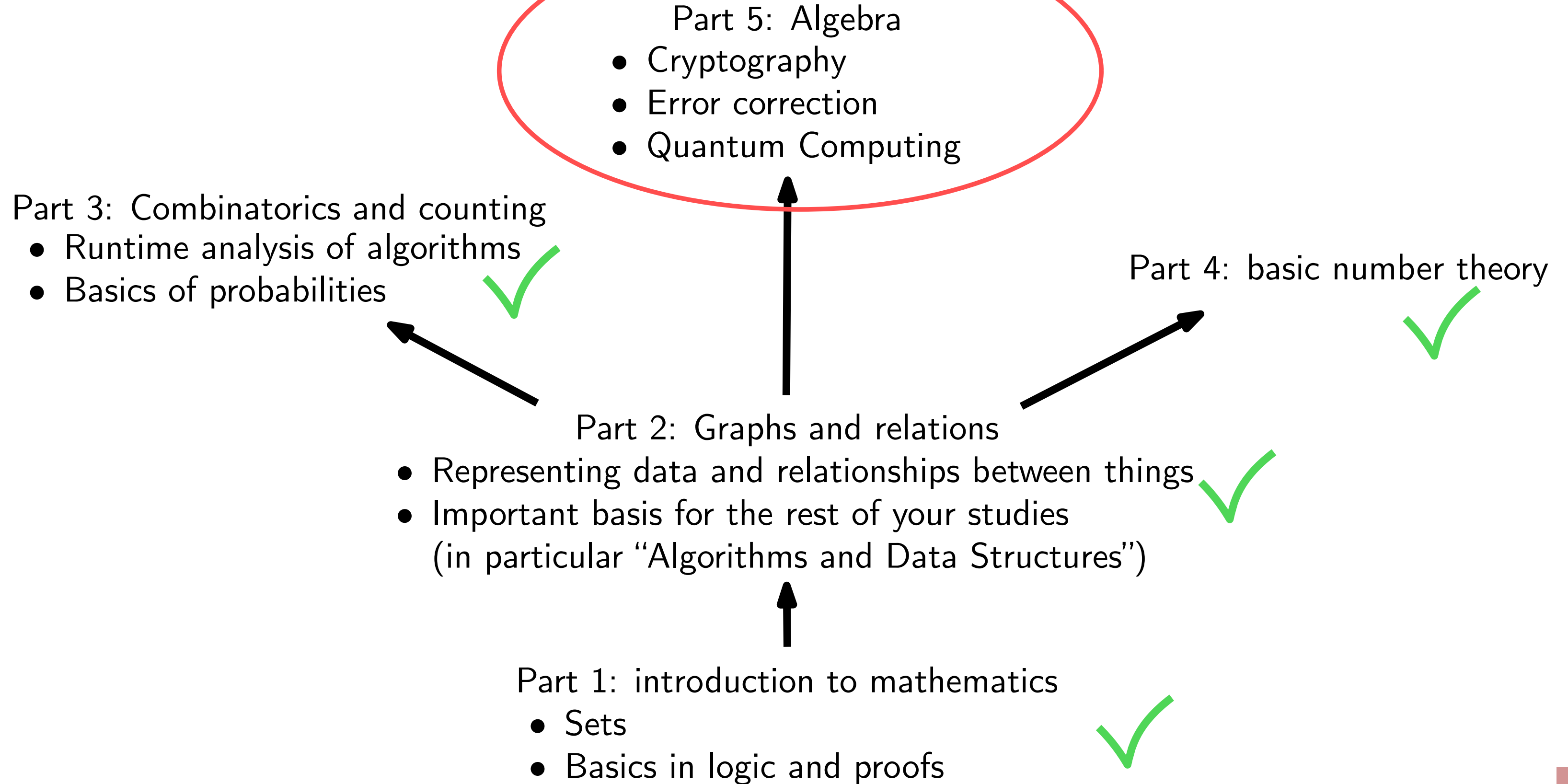
Theorem. RSA works: for all $M \in \mathbb{Z}/n\mathbb{Z}$, we have $(M^e)^d = M \bmod n$.

Want: n, e, d such that $(M^e)^d = M \bmod n$ for all $M \in \mathbb{Z}/n\mathbb{Z}$

Key generation:

- Choose **distinct prime numbers** p and q
- $n := pq$
- $e \in \{2, \dots, \varphi(n) - 1\}$ **coprime** with $\varphi(n)$
- d **inverse** of e modulo $\varphi(n)$

Theorem. RSA works: for all $M \in \mathbb{Z}/n\mathbb{Z}$, we have $(M^e)^d = M \bmod n$.



Algebra: study of **operations** and **equations** on *stuff*

Number theory

Numbers: $+$, \times , $1/x$, 1 , 0
 Matrices: $+$, \times , M^{-1} , I , 0

Linear algebra

Sets: \cap , \cup , \times , Δ , \emptyset , \dots
 Functions: \circ , f^{-1} , Id_A

Boolean algebra

Booleans: \wedge , \vee , \Rightarrow , \neg , \top , \perp
 Relations: \circ , R^T , Id , \cup , \cap , \times , \dots

Relational algebra

Modular arithmetic: $+$, \times , $[a]_d^{-1}$, $[1]_d$, $[0]_d$

Introduction to Abstract Algebra

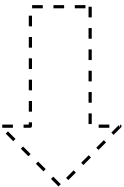
Abstract means not concrete

Abstract	Concrete
Structures with multiplication, neutral elements	Relations: \circ , Id
Structures with multiplication, inverses, neutral elements	Real Numbers: \times , $1/x$, 1 Matrices: \times , M^{-1} , I Bijective Functions: \circ , f^{-1} , Id_A Modular arithmetic: \times , $[a]_d^{-1}$, $[1]_d$
Structures with meet and join (and maximal/minimal elements)	Booleans: \wedge , \vee , \top , \perp Numbers: \wedge , \vee , 0 , 1

Abstract means not concrete

Abstract	Concrete
Structures with multiplication, neutral elements	Relations: \circ , Id
Structures with multiplication, inverses, neutral elements	Real Numbers: \times , $1/x$, 1 Matrices: \times , M^{-1} , I Bijective Functions: \circ , f^{-1} , Id_A Modular arithmetic: \times , $[a]_d^{-1}$, $[1]_d$
Structures with meet and join (and maximal/minimal elements)	Booleans: \wedge , \vee , \top , \perp Numbers: \wedge , \vee , 0 , 1

Concrete examples we want to study



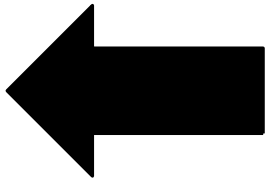
for example, Fermat's little theorem

General theorems about
all our examples

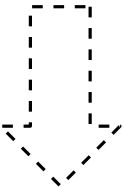
Abstract means not concrete

Abstract	Concrete
Structures with multiplication, neutral elements	Relations: \circ , Id
Structures with multiplication, inverses, neutral elements	Real Numbers: \times , $1/x$, 1 Matrices: \times , M^{-1} , I Bijective Functions: \circ , f^{-1} , Id_A Modular arithmetic: \times , $[a]_d^{-1}$, $[1]_d$
Structures with meet and join (and maximal/minimal elements)	Booleans: \wedge , \vee , \top , \perp Numbers: \wedge , \vee , 0 , 1

Definition of abstract object that generalizes something we know



Concrete examples we want to study



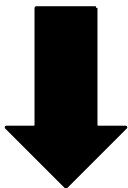
for example, Fermat's little theorem

General theorems about all our examples

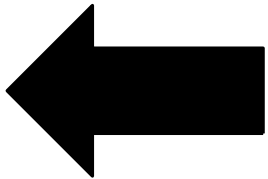
Abstract means not concrete

Abstract	Concrete
Structures with multiplication, neutral elements	Relations: \circ , Id
Structures with multiplication, inverses, neutral elements	Real Numbers: \times , $1/x$, 1 Matrices: \times , M^{-1} , I Bijective Functions: \circ , f^{-1} , Id_A Modular arithmetic: \times , $[a]_d^{-1}$, $[1]_d$
Structures with meet and join (and maximal/minimal elements)	Booleans: \wedge , \vee , \top , \perp Numbers: \wedge , \vee , 0 , 1

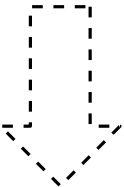
Definition of abstract object that generalizes something we know



Identify some properties that are important in the concrete case



Concrete examples we want to study



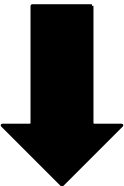
for example, Fermat's little theorem

General theorems about all our examples

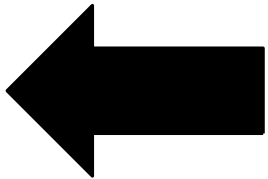
Abstract means not concrete

Abstract	Concrete
Structures with multiplication, neutral elements	Relations: \circ , Id
Structures with multiplication, inverses, neutral elements	Real Numbers: \times , $1/x$, 1 Matrices: \times , M^{-1} , I Bijective Functions: \circ , f^{-1} , Id_A Modular arithmetic: \times , $[a]_d^{-1}$, $[1]_d$
Structures with meet and join (and maximal/minimal elements)	Booleans: \wedge , \vee , \top , \perp Numbers: \wedge , \vee , 0 , 1

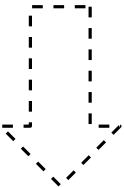
Definition of abstract object that generalizes something we know



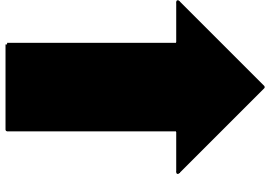
Identify some properties that are important in the concrete case



Concrete examples we want to study



for example, Fermat's little theorem



General theorems about all our examples

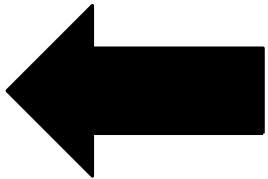
Abstract means not concrete

Abstract	Concrete
Structures with multiplication, neutral elements	Relations: \circ , Id
Structures with multiplication, inverses, neutral elements	Real Numbers: \times , $1/x$, 1 Matrices: \times , M^{-1} , I Bijective Functions: \circ , f^{-1} , Id_A Modular arithmetic: \times , $[a]_d^{-1}$, $[1]_d$
Structures with meet and join (and maximal/minimal elements)	Booleans: \wedge , \vee , \top , \perp Numbers: \wedge , \vee , 0 , 1

Definition of abstract object that we know

Tip: have many examples in mind to not be overwhelmed

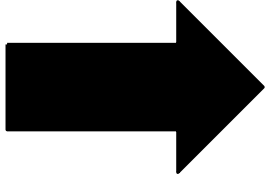
Identify some properties that are important in the concrete case



Concrete examples we want to study



for example, Fermat's little theorem



General theorems about all our examples

Definition. An **internal composition law** or **binary operation** on A is a function $\circ: A^2 \rightarrow A$.

We write $a \circ b$ instead of $\circ(a, b)$.

Definition. An **internal composition law** or **binary operation** on A is a function $\circ: A^2 \rightarrow A$.

We write $a \circ b$ instead of $\circ(a, b)$.

- If A is finite, a binary operation can be drawn by a **Cayley table**:

Definition. An **internal composition law** or **binary operation** on A is a function $\circ: A^2 \rightarrow A$.

We write $a \circ b$ instead of $\circ(a, b)$.

- If A is finite, a binary operation can be drawn by a **Cayley table**:

Example.

	a	b	c
a	a	b	c
b	b	c	a
c	c	b	b

- If A is infinite, we usually give some kind of formula:

Example. Law on \mathbb{N} : $n \circ m := nm + n + m + 1$
 $5 \circ 3 = 24$ $1 \circ 3 = 8$

Definition. An **internal composition law** or **binary operation** on A is a function $\circ: A^2 \rightarrow A$.

We write $a \circ b$ instead of $\circ(a, b)$.

- If A is finite, a binary operation can be drawn by a **Cayley table**:

Example.

	a	b	c
a	a	b	c
b	b	c	a
c	c	b	b

- If A is infinite, we usually give some kind of formula:

Example. Law on \mathbb{N} : $n \circ m := nm + n + m + 1$
 $5 \circ 3 = 24$ $1 \circ 3 = 8$

Only property to check: for every $a, b \in A$, $a \circ b$ is an element of A

Definition. An **internal composition law** or **binary operation** on A is a function $\circ: A^2 \rightarrow A$.

We write $a \circ b$ instead of $\circ(a, b)$.

- If A is finite, a binary operation can be drawn by a **Cayley table**:

Example.

	a	b	c
a	a	b	c
b	b	c	a
c	c	b	b

- If A is infinite, we usually give some kind of formula:

Example. Law on \mathbb{N} : $n \circ m := nm + n + m + 1$
 $5 \circ 3 = 24$ $1 \circ 3 = 8$

Only property to check: for every $a, b \in A$, $a \circ b$ is an element of A

For the following operations, decide if they are internal composition laws:

- Addition/Multiplication on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$
- Addition of vectors in \mathbb{R}^n
- Addition and multiplication of $n \times n$ matrices
- Composition of functions $A \rightarrow A$
- Subtraction of natural numbers
- Division of real numbers
- Scalar product in \mathbb{R}^n : $v \circ w = v_1 w_1 + v_2 w_2$

Definition. An **internal composition law** or **binary operation** on A is a function $\circ: A^2 \rightarrow A$.

We write $a \circ b$ instead of $\circ(a, b)$.

- If A is finite, a binary operation can be drawn by a **Cayley table**:
- If A is infinite, we usually give some kind of formula:

Example.

	a	b	c
a	a	b	c
b	b	c	a
c	c	b	b

Example. Law on \mathbb{N} : $n \circ m := nm + n + m + 1$
 $5 \circ 3 = 24$ $1 \circ 3 = 8$

Only property to check: for every $a, b \in A$, $a \circ b$ is an element of A

For $v, w \in \mathbb{R}^3$, define $v \wedge w := \begin{pmatrix} v_2 w_3 - v_3 w_2 \\ v_3 w_1 - v_1 w_3 \\ v_1 w_2 - v_2 w_1 \end{pmatrix}$.

Is \wedge an internal composition law on \mathbb{R}^3 ?



Definition. An **internal composition law** or **binary operation** on A is a function $\circ: A^2 \rightarrow A$.

We write $a \circ b$ instead of $\circ(a, b)$.

- If A is finite, a binary operation can be drawn by a **Cayley table**:
- If A is infinite, we usually give some kind of formula:

Example.

	a	b	c
a	a	b	c
b	b	c	a
c	c	b	b

Example. Law on \mathbb{N} : $n \circ m := nm + n + m + 1$
 $5 \circ 3 = 24$ $1 \circ 3 = 8$

Only property to check: for every $a, b \in A$, $a \circ b$ is an element of A

For $v \in \mathbb{R}^3$ and $\lambda \in \mathbb{R}^3$, define $\lambda \circ v := \begin{pmatrix} \lambda v_1 \\ \lambda v_2 \\ \lambda v_3 \end{pmatrix}$.
Is \circ an internal composition law on \mathbb{R}^3 ?



Definition. Let \circ be an internal composition law on A . We say that it:

- is **associative** if for all $a, b, c \in A$, we have $a \circ (b \circ c) = (a \circ b) \circ c$ (parentheses don't matter)
- is **commutative** if for all $a, b \in A$, we have $a \circ b = b \circ a$ (order doesn't matter)
- has a **neutral element** if there exists $e \in A$ such that for all $a \in A$, $e \circ a = a \circ e = a$

Definition. Let \circ be an internal composition law on A . We say that it:

- is **associative** if for all $a, b, c \in A$, we have $a \circ (b \circ c) = (a \circ b) \circ c$ (parentheses don't matter)
- is **commutative** if for all $a, b \in A$, we have $a \circ b = b \circ a$ (order doesn't matter)
- has a **neutral element** if there exists $e \in A$ such that for all $a \in A$, $e \circ a = a \circ e = a$

Notation (Multiplicative/Exponent notation). For $n > 0$: a^n : $a \circ \dots \circ a$.

Definition. Let \circ be an internal composition law on A . We say that it:

- is **associative** if for all $a, b, c \in A$, we have $a \circ (b \circ c) = (a \circ b) \circ c$ (parentheses don't matter)
- is **commutative** if for all $a, b \in A$, we have $a \circ b = b \circ a$ (order doesn't matter)
- has a **neutral element** if there exists $e \in A$ such that for all $a \in A$, $e \circ a = a \circ e = a$

Notation (Multiplicative/Exponent notation). For $n > 0$: a^n : $a \circ \dots \circ a$.

If \circ is commutative, we can use the additive notation instead:

Notation. Let $+$ be a **commutative** internal composition law on A . We define $n \cdot a$ by $a + \dots + a$.

Definition. Let \circ be an internal composition law on A . We say that it:

- is **associative** if for all $a, b, c \in A$, we have $a \circ (b \circ c) = (a \circ b) \circ c$ (parentheses don't matter)
- is **commutative** if for all $a, b \in A$, we have $a \circ b = b \circ a$ (order doesn't matter)
- has a **neutral element** if there exists $e \in A$ such that for all $a \in A$, $e \circ a = a \circ e = a$

(A, \circ) is a **monoid**: if \circ is associative and has a neutral element

commutative monoid: if \circ is associative, commutative, and has a neutral element

Definition. Let \circ be an internal composition law on A . We say that it:

- is **associative** if for all $a, b, c \in A$, we have $a \circ (b \circ c) = (a \circ b) \circ c$ (parentheses don't matter)
- is **commutative** if for all $a, b \in A$, we have $a \circ b = b \circ a$ (order doesn't matter)
- has a **neutral element** if there exists $e \in A$ such that for all $a \in A$, $e \circ a = a \circ e = a$

(A, \circ) is a **monoid**: if \circ is associative and has a neutral element

commutative monoid: if \circ is associative, commutative, and has a neutral element

Examples. The following are monoids:

- $(\mathbb{N}_0, +)$
- $(\mathbb{Z}, +)$
- (\mathbb{N}, \times)
- $(\{0, 1\}^*, \text{concat})$
- (A^A, \circ)
- ...

Definition. Let \circ be an internal composition law on A . We say that it:

- is **associative** if for all $a, b, c \in A$, we have $a \circ (b \circ c) = (a \circ b) \circ c$ (parentheses don't matter)
- is **commutative** if for all $a, b \in A$, we have $a \circ b = b \circ a$ (order doesn't matter)
- has a **neutral element** if there exists $e \in A$ such that for all $a \in A$, $e \circ a = a \circ e = a$

(A, \circ) is a **monoid**: if \circ is associative and has a neutral element

commutative monoid: if \circ is associative, commutative, and has a neutral element

Examples. The following are monoids:

- $(\mathbb{N}_0, +)$
- $(\mathbb{Z}, +)$
- (\mathbb{N}, \times)
- $(\{0, 1\}^*, \text{concat})$
- (A^A, \circ)
- ...

Theorem. Let \circ be an internal composition law. There can be **at most one** neutral element for \circ .

Definition. Let \circ be an internal composition law on A . We say that it:

- is **associative** if for all $a, b, c \in A$, we have $a \circ (b \circ c) = (a \circ b) \circ c$ (parentheses don't matter)
- is **commutative** if for all $a, b \in A$, we have $a \circ b = b \circ a$ (order doesn't matter)
- has a **neutral element** if there exists $e \in A$ such that for all $a \in A$, $e \circ a = a \circ e = a$

(A, \circ) is a **monoid**: if \circ is associative and has a neutral element

commutative monoid: if \circ is associative, commutative, and has a neutral element

Examples. The following are monoids:

- $(\mathbb{N}_0, +)$
- $(\mathbb{Z}, +)$
- (\mathbb{N}, \times)
- $(\{0, 1\}^*, \text{concat})$
- (A^A, \circ)
- ...

Let M be the set of all $n \times n$ matrices.
Is (M, \times) a monoid?



Theorem. Let \circ be an internal composition law.
There can be **at most one** neutral element for \circ .

Definition. Let (A, \circ) be a monoid and $a, b \in A$.
 b is an **inverse** of a if $a \circ b = b \circ a = e$.

(A, \circ) is a **group** if \circ is associative, has a neutral element, and **every** element of A has an inverse.
Intuition: elements in A represent actions that can be reversed

Definition. Let (A, \circ) be a monoid and $a, b \in A$.
 b is an **inverse** of a if $a \circ b = b \circ a = e$.

(A, \circ) is a **group** if \circ is associative, has a neutral element, and **every** element of A has an inverse.
Intuition: elements in A represent actions that can be reversed

Groups are extremely important in science:

- Quantum theory
- Quantum computing: allowed operations form a group
- Cryptography
- Discrete Fourier transform: Signal processing and other things
- Study of polynomial equations and their solutions

Definition. Let (A, \circ) be a monoid and $a, b \in A$.
 b is an **inverse** of a if $a \circ b = b \circ a = e$.

(A, \circ) is a **group** if \circ is associative, has a neutral element, and **every** element of A has an inverse.
Intuition: elements in A represent actions that can be reversed

Examples. The following are groups:

- $(\mathbb{R}, +)$
- $(\mathbb{Z}, +)$
- (bijective functions $A \rightarrow A, \circ$)
- $(\mathbb{Z}/3\mathbb{Z}, \times)$

Definition. Let (A, \circ) be a monoid and $a, b \in A$. b is an **inverse** of a if $a \circ b = b \circ a = e$.

(A, \circ) is a **group** if \circ is associative, has a neutral element, and **every** element of A has an inverse.
Intuition: elements in A represent actions that can be reversed

Examples. The following are groups:

- $(\mathbb{R}, +)$
- $(\mathbb{Z}, +)$
- (bijective functions $A \rightarrow A, \circ$)
- $(\mathbb{Z}/3\mathbb{Z}, \times)$

Is (\mathbb{R}, \times) a group?



Definition. Let (A, \circ) be a monoid and $a, b \in A$.
 b is an **inverse** of a if $a \circ b = b \circ a = e$.

(A, \circ) is a **group** if \circ is associative, has a neutral element, and **every** element of A has an inverse.
Intuition: elements in A represent actions that can be reversed

Examples. The following are groups:

- $(\mathbb{R}, +)$
- $(\mathbb{Z}, +)$
- (bijective functions $A \rightarrow A, \circ$)
- $(\mathbb{Z}/3\mathbb{Z}, \times)$

Theorem. Any $a \in A$ has **at most one** inverse.

Definition. Let (A, \circ) be a monoid and $a, b \in A$.
 b is an **inverse** of a if $a \circ b = b \circ a = e$.

(A, \circ) is a **group** if \circ is associative, has a neutral element, and **every** element of A has an inverse.
Intuition: elements in A represent actions that can be reversed

Examples. The following are groups:

- $(\mathbb{R}, +)$
- $(\mathbb{Z}, +)$
- (bijective functions $A \rightarrow A, \circ$)
- $(\mathbb{Z}/3\mathbb{Z}, \times)$

Theorem. Any $a \in A$ has **at most one** inverse.

- **The** inverse of a is written a^{-1} .
- Usual rules of exponentiation are true:
 $a^p = (a^{-p})^{-1}$ for $p < 0$

Definition. Let (A, \circ) be a monoid and $a, b \in A$.
 b is an **inverse** of a if $a \circ b = b \circ a = e$.

(A, \circ) is a **group** if \circ is associative, has a neutral element, and **every** element of A has an inverse.

Intuition: elements in A represent actions that can be reversed

Examples. The following are groups:

- $(\mathbb{R}, +)$
- $(\mathbb{Z}, +)$
- (bijective functions $A \rightarrow A, \circ$)
- $(\mathbb{Z}/3\mathbb{Z}, \times)$

Theorem. Any $a \in A$ has **at most one** inverse.

- **The** inverse of a is written a^{-1} .
- Usual rules of exponentiation are true:
 $a^p = (a^{-p})^{-1}$ for $p < 0$

Theorem. Let (A, \circ) be a **group**, and let a, b be such that $a \circ b = e$.
Then $b \circ a = e$. (So b is the inverse of a .)

- Quaternion group Q_8
 - elements are $\{1, -1, i, -i, j, -j, k, -k\}$
 - operation given by the table

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

- Quaternion group Q_8
 - elements are $\{1, -1, i, -i, j, -j, k, -k\}$
 - operation given by the table

Find the neutral element and the inverse of $-j$



	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

- Quaternion group Q_8
 - elements are $\{1, -1, i, -i, j, -j, k, -k\}$
 - operation given by the table

Find the neutral element and the inverse of $-j$

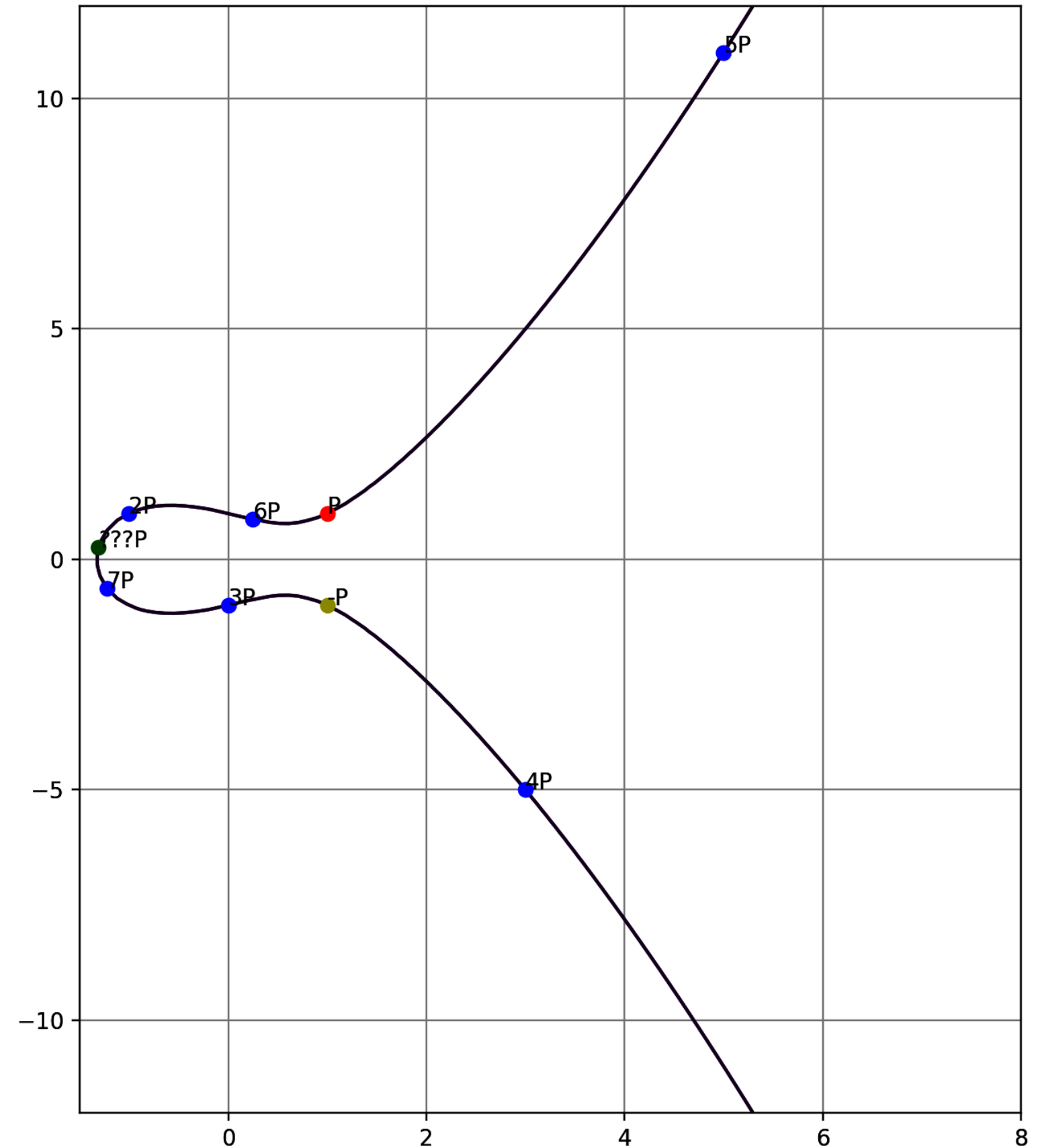


Applications: coordinates / movement in 3d.

- computer graphics
- motion planning for robots
- VR

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

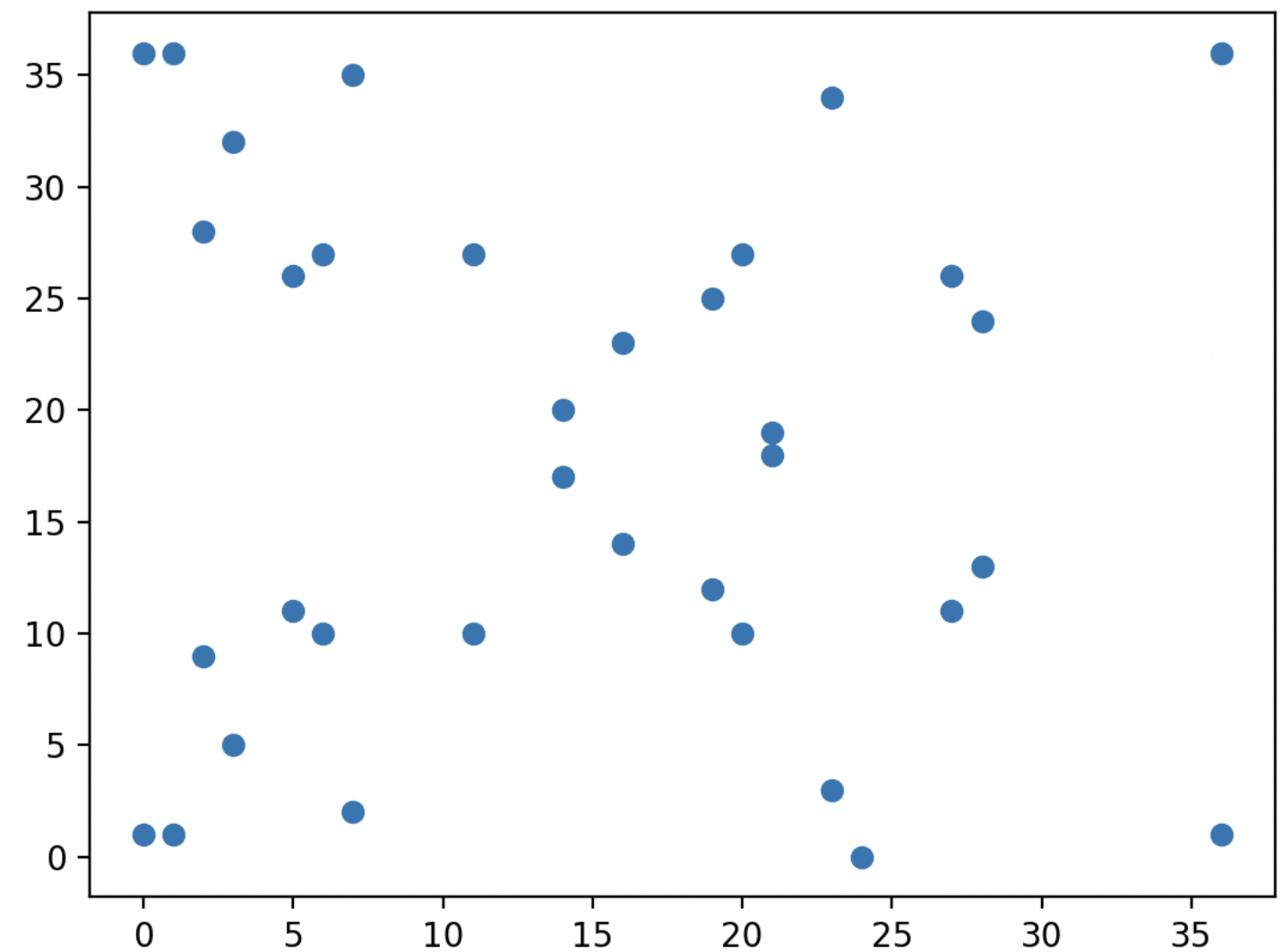
- Elliptic curves
 - elements: set of pairs (x, y) such that $y^2 = x^3 + ax + b$ (for some fixed a, b)
 - there is a way to “multiply” points
 - this is a commutative group



- Elliptic curves
 - elements: set of pairs (x, y) such that $y^2 = x^3 + ax + b$ (for some fixed a, b)
 - there is a way to “multiply” points
 - this is a commutative group

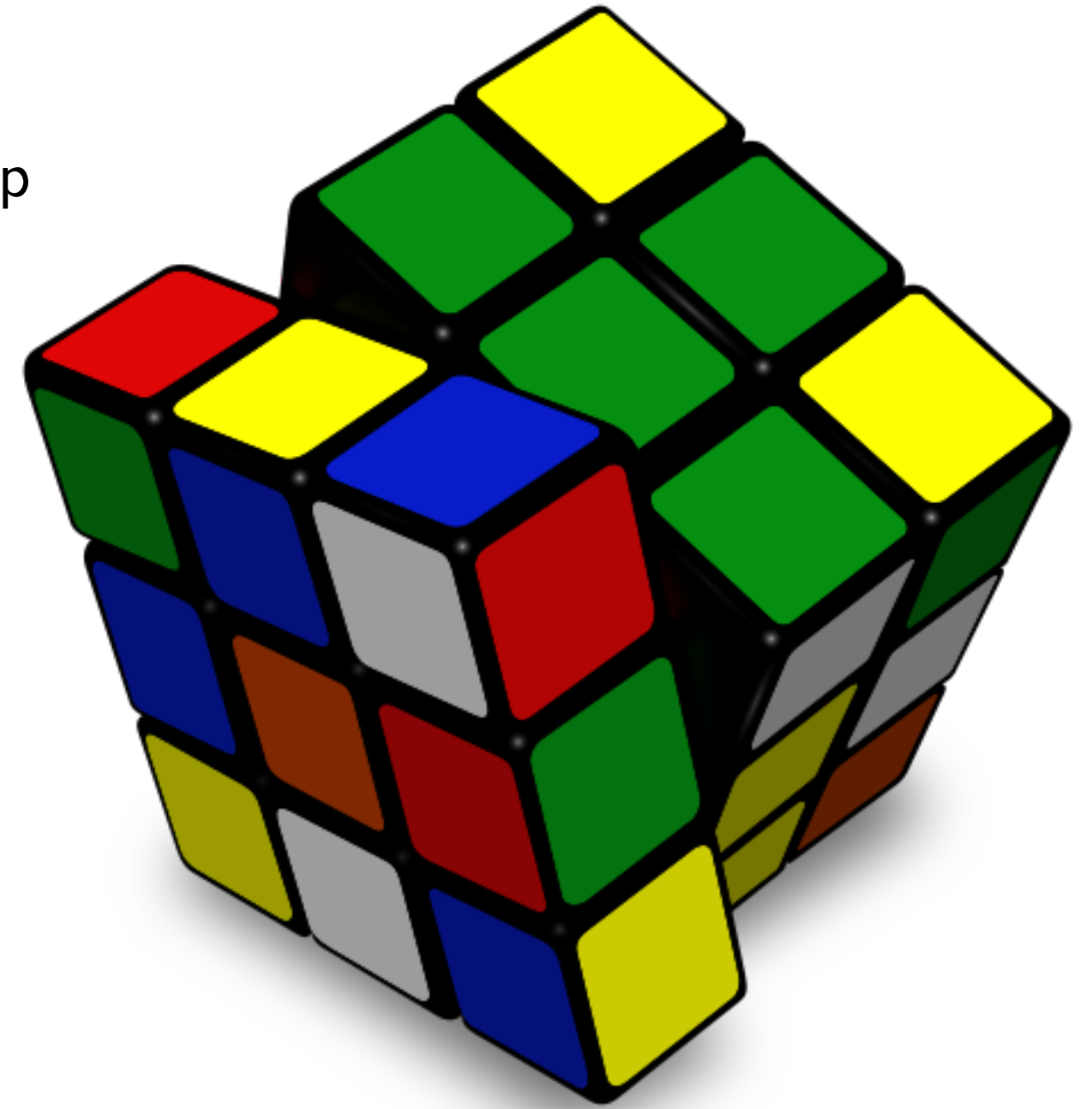
Application: elliptic curve cryptography

- Private key is an integer d
- Public key is the point $d \cdot P$



Points have coordinates in $\mathbb{Z}/37\mathbb{Z}$

- Rubik's cube
 - Elementary moves of the cube: F, B, U, D, L, R
 - Each position of the cube can be written as a sequence $FULR^{-1} \dots$ of moves starting from a solved cube
 - Each move can be “undone” \rightsquigarrow inverse elements \rightsquigarrow group
 - $|G| > 43 \times 10^{18}$



Theorem (Fermat's little theorem). If a and n are **coprime**, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Theorem (Fermat's little theorem). If a and n are **coprime**, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

What does it have to do with groups?

Theorem. Let U_n be the set of $[a] \in \mathbb{Z}/n\mathbb{Z}$ such that a **coprime** with n . Then (U_n, \times) is a group.

Theorem (Fermat's little theorem). If a and n are **coprime**, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

What does it have to do with groups?

Theorem. Let U_n be the set of $[a] \in \mathbb{Z}/n\mathbb{Z}$ such that a **coprime** with n . Then (U_n, \times) is a group.

Theorem. Let (G, \circ) be a **finite** group and $a \in G$. Then $a^{|G|} = e$.

Theorem (Fermat's little theorem). If a and n are **coprime**, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

What does it have to do with groups?

Theorem. Let U_n be the set of $[a] \in \mathbb{Z}/n\mathbb{Z}$ such that a **coprime** with n . Then (U_n, \times) is a group.

Theorem. Let (G, \circ) be a **finite** group and $a \in G$. Then $a^{|G|} = e$.

Step 1: For some $n > 0$, we have $a^n = e$

Theorem (Fermat's little theorem). If a and n are **coprime**, then $a^{\varphi(n)} = 1 \bmod n$.

What does it have to do with groups?

Theorem. Let U_n be the set of $[a] \in \mathbb{Z}/n\mathbb{Z}$ such that a **coprime** with n . Then (U_n, \times) is a group.

Theorem. Let (G, \circ) be a **finite** group and $a \in G$. Then $a^{|G|} = e$.

Step 1: For some $n > 0$, we have $a^n = e$

Step 2: define $b \sim c$ if $a^k \circ b = c$ for some $k \in \mathbb{Z}$

$a^3 \bullet$	$a^3 \circ b \bullet$	$a^3 \circ c \bullet$	$a^3 \circ d \bullet$
$a^2 \bullet$	$a^2 \circ b \bullet$	$a^2 \circ c \bullet$	$a^2 \circ d \bullet$
$a \bullet$	$a \circ b \bullet$	$a \circ c \bullet$	$a \circ d \bullet$
$e = a^4 \bullet$	$b \bullet$	$c \bullet$	$d \bullet$

Theorem (Fermat's little theorem). If a and n are coprime, then $a^{\varphi(n)} = 1 \bmod n$.

What does it have to do with groups?

Theorem. Let U_n be the set of $[a] \in \mathbb{Z}/n\mathbb{Z}$ such that a coprime with n . Then (U_n, \times) is a group.

Theorem. Let (G, \circ) be a finite group and $a \in G$. Then $a^{|G|} = e$.

Step 1: For some $n > 0$, we have $a^n = e$

Step 2: define $b \sim c$ if $a^k \circ b = c$ for some $k \in \mathbb{Z}$

Step 3: all equivalence classes have the same size

$a^3 \bullet$	$a^3 \circ b \bullet$	$a^3 \circ c \bullet$	$a^3 \circ d \bullet$
$a^2 \bullet$	$a^2 \circ b \bullet$	$a^2 \circ c \bullet$	$a^2 \circ d \bullet$
$a \bullet$	$a \circ b \bullet$	$a \circ c \bullet$	$a \circ d \bullet$
$e = a^4 \bullet$	$b \bullet$	$c \bullet$	$d \bullet$

Theorem (Fermat's little theorem). If a and n are **coprime**, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.



What does it have to do with groups?

Theorem. Let U_n be the set of $[a] \in \mathbb{Z}/n\mathbb{Z}$ such that a **coprime** with n . Then (U_n, \times) is a group.

Theorem. Let (G, \circ) be a **finite** group and $a \in G$. Then $a^{|G|} = e$.

The smallest $n > 0$ such that $a^n = e$ is called the **order** of a .

- definitions of associativity, commutativity, neutral element, inverses
- be able to check if some (A, \circ) is a monoid/group
- definition of the order of an element
- be comfortable with the notation

	associative	neutral element	inverses
monoid			
group	