Exercise 1 (Caesar's cipher ⋆)
Caesar's cipher is a monoalphabetic encryption method where all letters in the alphabet are shifted by a certain constant d. For example, with $d = 3$, we obtain

$$\texttt{A} \to \texttt{D},\ \texttt{B} \to \texttt{E},\ \ldots,\ \texttt{Y} \to \texttt{B},\ \texttt{Z} \to \texttt{C}.$$

1. Translate the encryption function f in algebraic terms. What is the decryption function g?
2. What is the *key* in Caesar's cipher? How many keys are possible?
3. Decrypt the ciphertext `LIPPSASVPH`.

Exercise 2 (Affine encryption ⋆)
We now want to study a more general kind of encryption method, called affine encryption. We represent each letter in the latin alphabet by its position in the alphabet, starting with 0, *i.e.*

$$\texttt{A} \to 0,\ \texttt{B} \to 1,\ \texttt{C} \to 2,\ \ldots,\ \texttt{Z} \to 25,$$

and we consider the map

$$f : x \to ax + b \mod 26,$$

where a and b are fixed integers between 0 and 25. We want to use the map f to encrypt each letter in the plaintext.

1. What happens if we choose $a = 1$?

We now choose $a = 10$ and $b = 3$.

2. Let $0 \leq y \leq 25$ such that $y = f(x) \overset{\text{def}}{=} 10x + 3 \mod 26$. Prove that there exists $k \in \mathbb{Z}$ such that $y = 10x + 26k + 3$.
3. Prove that y is always odd.
4. What can we say about this encryption method?

We now choose $a = 9$ and $b = 4$.

5. Find an integer $u \in \mathbb{Z}$ such that $9u = 1 \mod 26$.
6. Explain why the equation $y = 9x + 4 \mod 26$, with $0 \leq y \leq 25$, always has a solution.
7. What is the decryption function associated with $f(x) = 9x + 4$? How is decrypted the letter `E`?

Exercise 3 (The Vigenère cipher ⋆)
The Vigenère cipher is a cryptographic method using polyalphabetic substitution to encrypt text. It uses a word or multiple words that are repeated to form the key. Each letter in the latin alphabet is replaced by its position in the alphabet, starting with 0, *i.e.*

$$\texttt{A} \to 0,\ \texttt{B} \to 1,\ \texttt{C} \to 2,\ \ldots,\ \texttt{Z} \to 25.$$

Then, each letter in the plaintext is shifted by the number corresponding to the letter in the key. For example, the letter `C` in the plaintext encrypted using the letter `F` gives the letter `G` in the ciphertext.

More generally, if the number x is associated with the letter in the plaintext, y with the letter in the key, then the corresponding letter in the ciphertext is associated to the number

$$z = x + y \mod 26.$$

Here is another example with the key `PARIS` and the plaintext `COOLSUMMER`. It gives the ciphertext `ROFTKJMDMJ`. Table 1 can also be used to encrypt with the Vigenère cipher.

Plaintext	C	O	O	L	S	U	M	M	E	R
x	2	14	14	11	18	20	12	12	4	17
Key	P	A	R	I	S	P	A	R	I	S
y	15	0	17	8	18	15	0	17	8	18
z	17	14	5	19	10	9	12	3	12	9
Ciphertext	R	O	F	T	K	J	M	D	M	J

1. What cipher do we find if we use a one-letter key in the Vigenère cipher?
2. Encrypt the word `ARITHMETIC` using the key `MATH`.
3. Find the word corresponding to the ciphertext `UNYPZIMF`, still using the key `MATH`.
4. The sequences `TFUE` and `KA` can be found two times in the word `TFUEFKNFMTFUEKAAKBSKAEHNEJMIFG`. By analysing the distances between the identical sequences, deduce that the key is a 3-letters word.
5. We still consider the ciphertext `TFUEFKNFMTFUEKAAKBSKAEHNEJMIFG`. Can you find the original message? The most frequent letters in English are, from the most frequent to the least frequent: e, t, a, o, i, n, s, h and r.

Exercise 4 (RSA cryptosystem ⋆⋆)
The cryptosystem RSA is a public-key encryption method described by Rivest, Sharmir and Adleman in 1977. Let Alice and Bob be two persons that want to communicate: Alice wants to send a message to Bob. Bob chooses two prime numbers p and q, computes $n = pq$ and $\varphi(n) = (p-1)(q-1)$. Bob also chooses a number e such that e and $\varphi(n)$ are coprime, *i.e.* $\gcd(e, \varphi(n)) = 1$ and computes a number d such that $ed = 1 \mod \varphi(n)$. The pair (n, e) is then the *public key* whereas $(\varphi(n), d)$ is the *private key*.

Part A. Some equalities in the RSA cryptosystem can be obtained using *Fermat's little theorem*: if p is a prime number, and a an integer not divisible by p, then $a^{p-1} = 1 \mod p$.

1. Let a be an integer coprime with p and q, *i.e.* such that $\gcd(a, p) = \gcd(a, q) = 1$. Prove that
$$a^{p-1} = 1 \mod p \text{ and } a^{q-1} = 1 \mod q.$$
2. Prove that $a^{(p-1)(q-1)} = 1 \mod n$.
3. Prove that for any integer a and for an integer k such that $k = 1 \mod \varphi(n)$, then $a^k = a \mod n$.

Part B.

4. Explain why the equation $(E) : ex - \varphi(n)y = 1$ has solutions.
5. Let (x_0, y_0) be a solution of (E), prove that (x, y) is another solution of (E) if and only if $x = x_0 + k\varphi(n)$ and $y = y_0 + ke$ where $k \in \mathbb{Z}$ in an integer.
6. Prove that there is only one integer $d < \varphi(n)$ such that $ed = 1 \mod \varphi(n)$.

Part C.

7. From Parts A and B, deduce that for any integers a, b, if we have $b = a^e \mod n$, then we have $b^d = a \mod n$. What does it mean for our cryptosystem?

Exercise 5 (Hardness of RSA ⋆)
We keep the same notations as in Exercice 4. We often say that the RSA cryptosystem is based on the fact that it is hard in practice to factorize a big integer $n = pq$. Nevertheless, it seems that we only need to know $\varphi(n)$. In this exercise we will see that it is equivalent to know (p, q) or $\varphi(n) = (p-1)(q-1)$.

1. Assume that we know p and q, how can we compute $\varphi(n)$?

Now assume that we know n (because this is public) and $\varphi(n)$.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Table 1: Vigenère encryption table, also knows as *tabula recta*.

2. Express $p+q$ using n and $\varphi(n)$.
3. Develop the polynomial $(X-p)(X-q)$.
4. Prove that we can recover p and q.

Exercise 6 (RSA with the same n $\star\star$)
Assume that Alice and Bob are using public keys that share the same integer $n = pq$, but not necessarily the same exponents e_A and e_B used to encrypt.

1. Explain why Alice can decrypt the messages sent to Bob.
2. Assume that $\gcd(e_A, e_B) = 1$. Show that a third person *Eve* can decrypt the messages that are sent to both Alice and Bob.

Exercise 7 (RSA in a network $\star\star$)
We want to use RSA with a network of k persons.

1. How many prime numbers do we have to generate?
2. We would like to reduce this number. Thus we first generate a small set of prime numbers and we pick two prime numbers in this set for each user in the network, such that every user has a different key. Show how a user can eventually factorize another user key?
3. Show how someone can factorize all keys that have a common factor with another key.

Exercise 8 (Algebraic structures: finite fields $\star$)
The set $\mathbb{Z}/n\mathbb{Z}$ is called a *finite field* if every element $x \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$ is invertible. Prove that $\mathbb{Z}/n\mathbb{Z}$ is a finite field *if and only if* n is a prime number.

Exercise 9 (A formula for $\varphi(n)$ $\star\star$)
In this exercise we will find a useful formula for φ, Euler's totient function. Let p be a prime number and $n \in \mathbb{N}, n \geq 2$. Recall that $\varphi(n)$ counts the positive numbers up to n that are coprime to n and thus we also have $\varphi(n)$ is the number of elements in $(\mathbb{Z}/n\mathbb{Z})^\times$.

1. Prove that $\varphi(p) = p - 1$.
2. Let $k \geq 1$ an integer and let $x \in \mathbb{N}$ such that $\gcd(x, p^k) \neq 1$. What are the possible values for $\gcd(x, p^k)$?
3. Prove that $\varphi(p^k) = p^k - p^{k-1}$.
4. Let $n = \prod_{i=1}^{r} p_i^{e_i}$ be the factorization of n. Find a formula for $\varphi(n)$ (recall that φ is *multiplicative*).

Exercise 10 (Arithmetic in $\mathbb{Z}/n\mathbb{Z}$ $\star$)
Here are some properties that are useful in cryptography.

1. Using Bézout's identity, show that an element a is invertible in $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a, n) = 1$.
2. Show that if $a, b \in \mathbb{Z}/n\mathbb{Z}$ are invertible, then ab is also invertible.

Exercise 11 (Diffie-Hellman $\star$)
Alice and Bob want to use the Diffie-Hellman protocol using $p = 11$.

1. Find the smallest α such that α is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$
2. Assume that Alice chooses $a = 5$ and Bob chooses $b = 9$ as secret values for the Diffie-Hellman protocol. Find the common key of Alice and Bob using the element α found in the previous question.
3. Assume that Eve manages to get between Alice and Bob in the communication channel, so that Alice really sends messages to Eve and Bob really sends messages to Eve. Assume that Eve chooses $e = 4$ for her secret value in order to communicate both with Alice and Bob. Find the keys of Alice, Bob, and Eve.
4. Can Alice and Bob know that there is someone in the middle of their communication?