Cryptography lecture notes

Contents

Part I

Introduction to modern cryptography

Front page

Latest update: 12/02/2021.

This page contains some useful information related to the course and the lecture notes. Note that there are some useful buttons above the text, in particular one to download the notes as a well-formatted PDF, for offline use.

Prerequisites

The course assumes that you are familiar with previous maths courses from your degree. In particular, we will be using concepts from Probability theory and Discrete mathematics, and make extensive use of modular arithmetic. Refreshers for these topics can be found in Appendix C and Section 5.3.

Exercises

Besides the exercise lists that you will have for practices or seminars, these notes also have some exercises embedded into the explanations. These are mostly easy exercises, designed to be a sort of 'sanity check' before moving to the next topic. Hence, our recommendation is that you stop and think about every exercise you encounter in these notes, instead of rushing through the content. You might not always be able to write a full and formal solution, but make sure to get at least an intuition on each exercise before moving on.

SageMath

SageMath (often called just *Sage*) is a powerful computer algebra system that we will use during the course to illustrate many concepts. It follows the Python syntax, which you will be familiar with, and comes equipped with many functions that are useful for cryptography.

These notes will sometimes provide chunks of Sage code, so that you can play with some of the schemes that we will introduce. You are also encouraged to

try and implement other schemes, or use Sage to double-check your solutions to exercises.

There are two ways that you can use Sage:

- Download it from https://www.sagemath.org/download.html. This will allow you to run SageMath locally. It also comes packaged with a Jupyter-style notebook, for ease of use.
- Use it online at https://cocalc.com/app. This also comes in both terminal and notebook flavors. CoCalc has a freemium model, and in the free version you will get an annoying message telling you that your code will run really slow. Nevertheless, the free version is more than enough for the purpose of this course.

The documentation at https://doc.sagemath.org/ is pretty good, although most of the functions that we will use are self-explanatory.

Bibliography

1. Boaz Barak. An Intensive Introduction to Cryptography. *Available freely from* https://intensecrypto.org/public/.

2. Richard Crandall and Carl B Pomerance. *Prime numbers: a computational perspective*, volume 182. Springer Science & Business Media, 2006.

3. Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. CRC press, 2020.

4. Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

5. Mike Rosulek. The Joy of Cryptography, 2017. Available freely from http://web.engr.oregonstate.edu/~rosulekm/crypto.

Changelog

- 12/02/2021. Section 8 added. Some typos fixed in Sections 6, (public-key-encryption) and Appendix B.
- 05/02/2021. Section 7 and Appendix B added. Minor fixes in Section 6. CRT moved to Section 5.
- 26/01/2021. Section 6 and Appendices A and C.4 added.
- 21/01/2021. Minor fixes and additions in Sections 4 and 5.
- 18/01/2021. Remainder of Section 5 uploaded. Some typos fixed in Sections 3 and 4.
- 13/01/2021. Section 4 uploaded.

- 08/01/2021. Section 3 uploaded.
- 07/01/2021. Section 5.3 and refreshers in Appendix C added. Added code for LFSR. Some typos fixed in Sections 1 and 2.
- 04/01/2021. Sections 1 and 2 uploaded.

Notes written by Javier Silva, using Bookdown and pandoc.

Chapter 1

Introduction to security

We use cryptography on a daily basis: our wireless communications or web traffic are encrypted, companies protect their data with cryptographic algorithms, and so on. We all have a basic or intuitive understanding of how cryptographic algorithms work. In this chapter, we want to make this intuition more precise and give you tools to think about cryptographic algorithms more formally, and reason scientifically about security.

Therefore, in this section we will:

1. Introduce three basic principles of cryptographic algorithm design;
2. Introduce the notion of security parameter and security level.

1.1 What cryptography is and is not

Cryptography is a field that lies halfway between mathematics and computer science, and is occupied with building algorithms that protect communications in some way, for example ensuring privacy or integrity of a message sent through an insecure channel.

In this course, we will describe some of the most important cryptographic algorithms. They are the foundation for many security mechanisms and protocols that are part of the digital world. Thus, when you finish this course, you will have the basis to understand these mechanisms. But it is also important that you understand what is *not* covered in this course, and what are the limitations of what you will learn. In particular, a well-known course on cryptography[1] mentions three warnings that you should take into consideration:

[1] D. Boneh. Cryptography I, Coursera. Available at https://www.coursera.org/learn/crypto.

1. Cryptography is not the solution to all security problems;
2. Cryptography is not reliable unless implemented and used properly;
3. Cryptography is not something that you should try to invent yourself, as there are many and many examples of broken ad-hoc designs.

1.2 Fundamental security principles

Let us consider a common example. When we type our WiFi password to connect to a network, we are assuming that what we are doing is "secure" because only us have some secret information (the password), that allows us to do this. In the context of cryptography, we call this secret information the *secret key*.

But what if an attacker tries all the possible keys until he finds the right one? This is what is called a *brute-force attack*. We will consider a few different scenarios:

- Our secret key is a 4-digit number. Then, in the worst case, the attacker will need to try
$$10^4 = 10000$$
potential keys. Assuming one try per second, this will take a bit less than three hours.
- Our secret key is a 12-character string of digits and English letters. Since there are 10 possible digits and 26 possible letters for each position, the number of potential keys is
$$36^{12} = 4738381338321616896.$$
At the same rate, the attacker will need, approximately, $1.5 \cdot 10^{11}$ *years* to try all of them. For reference, this number is roughly half of the number of stars in the Milky Way.

Exercise 1.1. *A WiFi password is* 10 *bits long. Assume that an attacker tries one password per second. How long does it take to find the key by brute force? What if the password is* λ *bits long?*

The idea is that, if our password is generated in a good way, this will take too long! So we are implicitly thinking that our scheme is secure because an attacker has limited time or limited money to buy hardware to perform very fast attacks and find our password. This leads to the first fundamental principle of modern cryptography:

Principle 1. *Security depends on the resources of the attacker. We say that a cryptographic scheme is secure if there are no efficient attacks.*

Cryptographic algorithms need to be carefully reviewed by the scientific community, and directions for implementation and interoperability must be given before they are adopted. This is done by institutions such as NIST, the National Institute of Standards and Technology in the US.[2] Thus, coming up with new, secure algorithms is difficult. In fact, the algorithms that are used in practice are public, known to everyone, and in particular to potential attackers. For instance, in the case of a WiFi password, it is a publicly-known fact that WPA is used. This is a general design principle in cryptography: security must come from the choice of a secret key and not from attackers not knowing which algorithm we are using.

Principle 2 (Kerckhoffs's principle). *Design your system so that it is secure even if the attacker knows all of its algorithms.*[3]

So what makes our systems secure is the fact that, although the attacker knows the algorithm, it does not know the secret key that we are using. Back to the WiFi example, an attacker knows that the WPA standard is used, but they just don't know our password.

Another implicit assumption that we are making when we think that our connection is "secure" is that our secret key is *sufficiently random*, that is, that there are *many possibilities* for the secret key. This leads us to the third and last principle.

Principle 3. *Security is impossible without randomness.*

As we will see, randomness plays an essential role in cryptographic algorithms. In particular, it is always essential that secret keys are chosen to be sufficiently random (i.e. they should have enough entropy). A bad randomness source almost always translates into a weakness of the cryptographic algorithm.

1.3 Security parameter

Obviously, cryptographic algorithms need to be efficient to be used in practice. On the other hand, we have seen that no attack should be efficient at all, i.e. they should be *computationally infeasible*. Before we go on, we need to determine the meaning of efficiency, so that the concept is formal and quantifiable. At the same time, and because of Principle 1, we need to relate efficiency with security somehow.

The way to achieve this is through a natural number that we call the *security parameter*, usually denoted by λ. The information about both security and efficiency will be expressed in terms of the security parameter.

[2] https://www.nist.gov/.

[3] *Kerckhoffs's principle is named after Auguste Kerckhoffs, who published the article* La Cryptographie Militaire* in 1883.*

Definition 1.1. *An algorithm $\mathcal{A}$ is said to be* efficient *(or* polynomial-time*) if there exists a positive polynomial p such that, for any $\lambda \in \mathbb{N}$, when $\mathcal{A}$ receives as input a bitstring of length λ, it finishes in $p(\lambda)$ steps.*

We note that here we are interested in having a rough estimate on the running time, so we count each basic bit operation as one step. We use equivalently the terms *running time*, *number of steps*, *number of operations*.

An important observation is that a *single polynomial* must work for any value of λ. Otherwise, any algorithm would be considered efficient. The intuition behind the definition is that we allow the running time of the algorithm to grow when the input gets larger, but not "too much too fast". Let us consider two examples to illustrate the concept of polynomial-time algorithms:

- Algorithm $\mathcal{A}$ takes two λ-bit integers m, n and adds them.
- Algorithm $\mathcal{B}$ takes a λ-bit integer $n \in \{0, \ldots, 2^\lambda - 1\}$ and finds its prime factors in the following way: for each $i = 1, \ldots, n$, it checks whether i divides n, and if that is the case it outputs i.

Are they efficient? The first one is efficient, because the number of operations is $O(\lambda)$, while the second one is inefficient because the number of operations is $O(2^\lambda)$. In other words, the number of operations grows *exponentially* when we increase the size of the input. As is well known, exponential functions grow much faster than polynomials, and so in this case we will not be able to find a polynomial to satisfy Definition 1.1. Thus, algorithm $\mathcal{B}$ is not efficient.

Below, you can find a Sage implementation of each of the two algorithms, with the tools to compare their running times for different sizes of λ. Observe that, by increasing the security parameter, soon the second algorithm starts taking too long to terminate.

```
# Choose the security parameter
sec_param = 12

# Generate two random numbers of bit length lambda
n = randrange(2^(sec_param-1),2^(sec_param)-1)
m = randrange(2^(sec_param-1),2^(sec_param)-1)

print ("n =",n,"\nm =",m)

# Define algorithm A, which adds the two numbers
def algorithm_a(n,m):
    n+m

# Measure the time it takes to run algorithm A
```

```
%time algorithm_a(n,m)

# Define algorithm A, which tries to factor a number
def algorithm_b(n):
    for i in range(1,n+1):
        if mod(n,i)==0:
            i

# Measure the time it takes to run algorithm B
%time algorithm_b(n)
```

Exercise 1.2. *Decide whether the following algorithms run in polynomial time:*

- *An algorithm that takes as input two integers n, m (in base 2) and computes the sum $n + m$.*
- *An algorithm that takes as input an integer n and prints all the integers from 1 to ℓ, if:*
  - $\ell = n$.
  - $\ell = n/2$.
  - $\ell = \sqrt{n}$.
  - $\ell = 10^6$.
  - $\ell = \log_2 n$.

We are now in position to discuss the efficiency and security of a cryptographic scheme in more grounded terms. For cryptographic schemes that require secret keys, the security parameter λ is the bit length of the key. All the algorithms that compose some cryptographic scheme, like an encryption or signature scheme, should run in time polynomial in λ.

A classical example of this is an encryption scheme, which is the cryptographic primitive that will be the focus of most of the course. We first introduce the notion of symmetric encryption scheme.[4]

Definition 1.2. *A* symmetric encryption scheme *is composed of three efficient algorithms:*

$$(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}).$$

- *The* KeyGen *algorithm chooses some key* k *of length λ, according to some probability distribution.*

[4] In the second half of the course, we will deal with the notion of *asymmetric encryption schemes*, in which there are two different keys, a *public key* that is used for encryption and a *secret key* that is used for decryption.

- *The* Enc *algorithm uses the secret key* k *to encrypt a message* m*, and outputs the encrypted message*

$$\mathsf{c} = \mathsf{Enc}_{\mathsf{k}}(\mathsf{m}).$$

- *The* Dec *algorithm uses the secret key* k *to decrypt an encrypted message* c*, recovering*

$$\mathsf{m}$$

as

$$\mathsf{Dec}_{\mathsf{k}}(\mathsf{c}) = \mathsf{m}.$$

In this context, m *is called the* plaintext*, and* c *is said to be its corresponding* ciphertext*.*

Technically, the fact that the algorithms are efficient is expressed as requiring that the three algorithms run in time polynomial in λ.[5]

On the other hand, observe that, if an attacker wants to try all the possible secret keys, it needs $O(2^\lambda)$ steps to do so. This is not polynomial time in the security parameter (again, it is exponential), so it is not efficient according to Definition 1.1.

1.4 Security level

Ideally, we would like that the best possible attack against a scheme is a brute-force attack, in which an attacker (also called *adversary*) needs to try all the possibilities. However, very often there exist much more sophisticated attacks that need less time. This motivates the following definition:

Definition 1.3. *A cryptographic scheme has* n-bit security *if the best known attack requires* 2^n *steps.*

When the best known attack is a brute-force attack, then $n = \lambda$, but we will see many examples of the opposite, which makes n significantly smaller. In a few lessons, we will see the example of hash functions, for which, in the best case,

$$n = \frac{\lambda}{2}.$$

If we require a security level of 80 bits, this forces us to choose $\lambda = 160$, at the least. Another example is RSA, which is a famous encryption scheme that we

[5] In many cryptography books, you will find that KeyGen should be a (probabilistic) polynomial time algorithm that takes as input 1^λ, which is the string with λ ones. This is a way to write that KeyGen should be polynomial in λ.

will study later in the course. In that case, λ needs to be 1024 to achieve a security level of roughly 80 bits.

Although all the algorithms that compose a scheme, like $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ in the encryption case, are still efficient, their running time typically increases with λ. The impact of this is that, the higher the value of λ, the more expensive the computations are.

But what is a good security level? Suppose you have some cryptographic algorithm that has n-bit security for key length λ. How do you decide what n is appropriate for your scheme to be secure? How is n to be chosen so that it is *infeasible* (i.e. inefficient for an adversary) to recover the key?

There is no unique answer to this question. As we saw in Principle 1, security is a matter of resources. If an adversary needs to use computational power to perform 2^n steps to attack your system, this will cost him money (electric power, hardware, etc). If your cryptographic tools are protecting something that is worth only 10€, an attacker will not be willing to spend a lot of money attacking it. RFID tags are a good example of this. On the other hand, if you are protecting valuable financial information, or critical infrastructure, you would better make sure that this costs the adversary a *lot* of resources.

A general rule of thumb is that a cryptosystem is expected to give you at the very least an 80-bit security level. By today's computing power levels, this is considered even a bit weak, and acceptable security levels are more around the 100-bit mark. This does not mean that any attack below 2^{100} can be easily run on your PC at home! The website https://www.keylength.com/ maintains a list of key size recommendations suggested by different organizations.

The following table, taken from Mike Rosulek's book *The Joy of Cryptography* gives some estimates of computational cost in economic terms.[6]

Security level	Approximate cost	Reference
50	$3.50	cup of coffee
55	$100	decent tickets to a Portland Trailblazers game
65	$130000	median home price in Oshkosh, WI
75	$130 million	budget of one of the Harry Potter movies
85	$140 billion	GDP of Hungary
92	$20 trillion	GDP of the United States
99	$2 quadrillion	all of human economic activity since 300,000 BC
128	really a lot	a billion human civilizations' worth of effort

[6]Note that he uses the English definition of billion, that is, 10^9. Same for the other amounts. Also, the table seems to be based on data from 2018, so the up-to-date numbers might vary slightly.

Exercise 1.3. *Determine the security level when:*

- *My password consists of* 20 *random letters of the Catalan alphabet.*
- *Same as above, but including also capital letters.*
- *My password is a word of the Catalan dictionary (88500 words).*

Part II

Symmetric cryptography

Chapter 2

Randomness in cryptography

As we saw above, and made explicit in Principle 3, we require randomness to guarantee secure cryptography. In this section, we will give some thought to how to obtain this randomness in the first place, and what to do when we do not have enough of it. As a motivating example, we will start by describing a well-known encryption scheme.

We will learn about:

1. The one-time pad encryption scheme;
2. Pseudorandom generators;
3. Sources of randomness.

2.1 One-time pad

The *one-time pad (OTP)* is an old encryption scheme, which was already known in the late 19th century, and was widely used in the 20th century for many military and intelligence operations.

The idea is extremely simple. Let us first recall the *exclusive or* (XOR) logic operation. Given two bits $b_0, b_1 \in \{0,1\}$, the operation is defined as

$$\mathsf{XOR}(b_0, b_1) = b_0 \oplus b_1 = \begin{cases} 0 & \text{if } b_0 = b_1, \\ 1 & \text{if } b_0 \neq b_1. \end{cases}$$

Equivalently, the operation corresponds to the following truth table:

b_0	b_1	$b_0 \oplus b_1$
0	0	0
0	1	1
1	0	1
1	1	0

We extend the notation to bitstrings of any length, i.e., given two bistrings $\mathbf{b}_0$ and $\mathbf{b}_1$ of the same length, we define

$$\mathbf{b}_0 \oplus \mathbf{b}_1$$

to be the bistring that results from XOR'ing each bit of $\mathbf{b}_0$ with the bit in the same position of $\mathbf{b}_1$.

Assume that Alice wants to send an encrypted message to Bob. The one-time pad works as follows. Key generation consists of choosing as a secret key a uniformly random bitstring of length λ as the key:

$$\mathsf{k} = k_1 k_2 \dots k_\lambda.$$

We denote this process by $\mathsf{k} \leftarrow \{0,1\}^\lambda$. Let m be a message that Alice wants to encrypt, written as a bitstring[1]

$$\mathsf{m} = m_1 m_2 \dots m_\lambda$$

of the same length. Then, the one-time pad encryption scheme works by XOR'ing each message bit with the corresponding key bit. More precisely, for the ith bit of the message, we compute

$$\mathsf{c} = \mathsf{m} \oplus \mathbf{k},$$

which is sent to Bob. Note that, because the XOR operation is its own inverse, the decryption algorithm works exactly like encryption. That is, Bob can recover the message by computing

$$\mathsf{m} = \mathsf{c} \oplus \mathsf{k}.$$

The first property that we want from any encryption scheme is *correctness*, which means that for any message m and any key k, we have that

$$\mathsf{Dec}_\mathsf{k}(\mathsf{Enc}_\mathsf{k}(\mathsf{m})) = \mathsf{m},$$

that is, if we encrypt and decrypt, we should recover the same message. Otherwise Alice and Bob will not be able to communicate.

[1] If the message is written with a different set of characters, like English letters, it is first processed into a bitstring, e.g. by associating to each letter its ASCII code in binary (https://en.wikipedia.org/wiki/ASCII).

Proposition 2.1. The one-time pad is a correct encryption scheme.

Proof. Using the definitions of encryption and decryption, we have that

$$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = \mathsf{Dec}_k(m \oplus k) = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus \mathbf{0} = m,$$

where $\mathbf{0}$ means the string of zeroes of size λ. In the last two steps, we used, respectively, that XOR'ing any string with itself produces $\mathbf{0}$, and that XOR'ing any string with $\mathbf{0}$ does not change the string.

□

Here is a straightforward implementation of the one-time pad. In this example, we want to send a message with 12 ASCII characters, so each character will require 8 bits. Thus, we choose a key length of 96.

```
from sage.crypto.util import ascii_integer
from sage.crypto.util import bin_to_ascii

# Set a security parameter
sec_param = 96

# Define the XOR operation:
def xor(a,b):
    return mod(int(a)+int(b),2) # You will learn why this is equivalent
                                # to XOR later in the course

### KEY GENERATION
# Generate a random key of length sec_param
k = random_vector(GF(2),sec_param)

### ENCRYPTION
# Choose a message
m = "Hello there."
# Process the message into a bitstring
m_bin = str(BinaryStrings().encoding(m))

# Encrypt the message bit by bit
c = ""
if (len(m_bin)<=sec_param):
    for i in range(len(m_bin)):
        c += str(xor(m_bin[i],k[i]))
    print("Ciphertext: "+c)
else:
    print("Message too long. Need a longer key.")
```

```
### DECRYPTION
# We use the same ciphertext obtained in the encryption part.

# Decrypt the ciphertext bit by bit
m_bin = ""
if (len(c)<=sec_param):
    for i in range(len(c)):
        m_bin += str(xor(c[i],k[i]))
    print("Plaintext: "+bin_to_ascii(m_bin))
else:
    print("Ciphertext too long. Need a longer key.")
```

The one-time pad receives its name from the fact that, when the key is used only once, the scheme has *perfect secrecy*. This means that the ciphertext produced reveals absolutely no information about the underlying plaintext, besides its length. We formalize this by saying that, given a ciphertext and two messages, the ciphertext has the same probability of corresponding to each of the messages.

Definition 2.1. *An encryption scheme has* perfect secrecy *when, for a uniformly random key* k*, all ciphertexts* c *and all pairs of messages* $\mathsf{m}_0, \mathsf{m}_1$*,*

$$\Pr[\mathsf{c} = \mathsf{Enc}_\mathsf{k}(\mathsf{m}_0)] = \Pr[\mathsf{c} = \mathsf{Enc}_\mathsf{k}(\mathsf{m}_1)].$$

Intuitively, the perfect secrecy of the OTP stems from these two observations:

- Look again at the truth table of the XOR operation, and observe that a 0 in the plaintext could equally come from a 0 or a 1 in the plaintext, depending on the key bit. Similarly, a 1 in the ciphertext could also come from a 0 or a 1 in the plaintext. In other words, if the key is chosen uniformly at random, each bit of the ciphertext has a probability of 1/2 of coming from a 0, and a probability 1/2 of coming from a 1.
- Because of the above, an adversary that intercepts a ciphertext $c_1 c_2 \dots c_\lambda$ cannot know the corresponding plaintext, as any given plaintext can be encrypted to *any* bitstring of length λ. In other words, for every ciphertext c and every message m, there exists a key k and a message such that

  $$\mathsf{Enc}_\mathsf{k}(m) = \mathsf{c} \qquad \text{and} \qquad \mathsf{Dec}_\mathsf{k}(\mathsf{c}) = m.$$

  So any ciphertext could correspond to any message, and there is no way to do better, regardless of the computational power of the attacker!

We formalize the above discussion in the following result.

Proposition 2.2. The one-time pad encryption scheme has perfect secrecy.

Proof. By the discussion above, we have that for any key k, message m and ciphertext c,

$$\Pr[\mathsf{c} = \mathsf{Enc}_{\mathsf{k}}(\mathsf{m})] = \frac{\#\{\text{keys } \mathsf{k} \text{ such that } \mathsf{c} = \mathsf{Enc}_{\mathsf{k}}(\mathsf{m})\}}{\#\{\text{possible keys}\}} = \frac{1}{2^{\lambda}}.$$

□

Exercise 2.1. *We said above that for every message* m *and any ciphertext* c*, there is always exactly one key* k *such that*

$$\mathsf{Enc}_{\mathsf{k}}(m) = \mathsf{c} \qquad \textit{and} \qquad \mathsf{Dec}_{\mathsf{k}}(\mathsf{c}) = m.$$

For arbitrary m *and* c*, which is that key, expressed in terms of* m *and* c*?*

This is all well and good, but obviously there's a catch. While the security of one-time pad is as good as it gets, it is simply impractical for a very simple reason: we need a key as large as the message, and moreover, we need a new key for each message. Moreover, if we want perfect secrecy, this is unavoidable.

Proposition 2.3. Any encryption scheme with perfect secrecy requires a key that is as long as the message, and it cannot be reused.

One reason that highlights how reusing keys in OTP breaks perfect secrecy is the following. Assume that we use the same key k for two messages $\mathsf{m}_0, \mathsf{m}_1$. Then, an attacker intercepts the ciphertexts

$$\mathsf{c}_0 = \mathsf{m}_0 \oplus \mathsf{k}, \qquad \mathsf{c}_1 = \mathsf{m}_1 \oplus \mathsf{k}.$$

The adversary can compute

$$\mathsf{c}_0 \oplus \mathsf{c}_1 = (\mathsf{m}_0 \oplus \mathsf{k}) \oplus (\mathsf{m}_1 \oplus \mathsf{k}) = \mathsf{m}_0 \oplus \mathsf{m}_1 \oplus (\mathsf{k} \oplus \mathsf{k}) = \mathsf{m}_0 \oplus \mathsf{m}_1 \oplus \mathbf{0} = \mathsf{m}_0 \oplus m_1.$$

That is, the adversary can get the XOR result of the two messages. Even if they do not know any of the messages on their own, this leaks partial information (e.g. a 0 in any position means that the two messages have the same value on that position).

So it's clear that for OTP to work we need keys as long as the messages, and there is no way around that. But how much of a big deal is that? An issue that we have not addressed yet is the fact that, for any of this to happen, the two parties involved need to agree on a common key k, that must remain secret for anyone else. If an insecure channel is the only medium for communication available:

- they cannot share the key unencrypted, since an attacker could be listening, and grab the key to decrypt everything that comes afterwards.

- they cannot encrypt the key, since they don't have a shared key to use encryption yet!

Later in the course, we will see that there are ways to securely share a key over an insecure channel. But for now, it suffices to say that these methods exist. However, sharing a new key of the size of the message, and a new one for each message, is simply not practical most of the time. Imagine the key sizes for sending audio or video over the Internet. This, ultimately, is what kills the one-time pad.

2.2 Pseudorandom generators

Before we move on, let us see if there is still some hope for the one-time pad. What if we start from a short uniformly random key k, and try to expand it to a longer key?

Let us assume that Alice and Bob wish to communicate using the one-time pad, and Alice wants to send a message of length h. But they have only shared a key $\mathsf{k} \in \{0,1\}^\ell$, for some $\ell < h$, so they proceed as follows:

1. They agree on a public function

   $$G : \{0,1\}^\ell \to \{0,1\}^h.$$

   That is, G receives a bitstring of length ℓ and outputs another of length h.

2. Since the function is deterministic, they can both compute

   $$\mathsf{k}' = G(\mathsf{k})$$

   on their own. Now they both know $\mathsf{k}' \in \{0,1\}^h$.

3. They use the one-time pad with key k'.

Observe that, since they have already "stretched" the key once, they could potentially take parts of k' and apply the function G again to generate new keys on demand. The scheme that results from stretching the randomness of a short shared key to an arbitrary length and encrypt the message through the XOR operation is known as a *stream cipher*. The initial key used is called the *seed*, and the subsequent keys generated are called the *key stream*.

The function G must be deterministic, otherwise Alice and Bob will not arrive at the same key, and they will not be able to communicate. Also note that, although G is public, k is not, so an attacker has no way of learning the new key k'.

However, there are some caveats to this. Since the input of the function is a set of size 2^ℓ, there are at most 2^ℓ outputs, whereas if we had used a uniformly random key of length h, we would have 2^h potential keys. Recall that perfect secrecy strongly relied on the keys being uniformly random, which clearly will not be the case here.

But, what if the output of G looks "close enough" to random? By this, we mean that no efficient algorithm can distinguish the output distribution of G and the uniform distribution in $\{0,1\}^h$. Then, if an adversary cannot tell that we are using a non-uniform distribution, they will not be able to exploit this fact in their attacks, and so our scheme will remain secure. Is any function G good enough for our purposes?

Exercise 2.2. *Consider the stream cipher presented above, with the following choices for the function G, for $h = 2\ell$.*

1. *G outputs a string of 2ℓ zeroes.*
2. *G outputs the input, followed by a string of ℓ zeroes.*
3. *G outputs two concatenated copies of the input.*

In each of these cases, discuss whether the scheme is still secure.

The above exercise shows that we need to be careful when choosing our function G. This leads us to the following definition.

Definition 2.2. *A* pseudorandom number generator (PRNG) *is a function*

$$G : \{0,1\}^\ell \to \{0,1\}^h$$

such that no efficient adversary can distinguish the output distribution of G from the uniform distribution on $\{0,1\}^h$.

We emphasize the importance of randomness here. A function G whose output cannot be distinguished from uniform randomness by any (efficient) algorithm implies that, for all practical purposes, the output of G can be considered uniformly random in $\{0,1\}^h$. In particular, informally this means that a key stream generated with a PRNG is *unpredictable*, i.e., given some output bits of G, there is no way to predict the next in polynomial time, with a success rate higher than 50%. This contrasts with non-cryptographic PRNGs, in which it is enough that the output passes some statistical tests, but might not be completely unpredictable.

Exercise 2.3. *Assume that there is a very bad PRNG that outputs one bit at a time, and that bit is a 0 with probability 3/4. This PRNG is used in a stream cipher to produce a ciphertext*

$$c = 01.$$

In OTP, the probability of the corresponding plaintext being 00*,* 01*,* 10 *or* 11 *would be* $1/4$ *each. Compute the corresponding probabilities when the bad PRNG described above is in use.*

An interesting property of PRNGs is that, if we manage to build one that stretches the key by just a little, then we can produce an infinitely large key stream, and still maintain essentially the same security guarantees. To illustrate this, let us again consider a function

$$G : \{0,1\}^\ell \to \{0,1\}^{2\ell},$$

and let us assume that it is a PRNG.[2] Consider the following construction of a new function

$$H : \{0,1\}^\ell \to \{0,1\}^{3\ell},$$

which works as follows: on input k,

1. First compute $G(\mathsf{k}) \in \{0,1\}^{2\ell}$.
2. Split the result in two halves $\mathbf{x}, \mathbf{y}$, each of length ℓ.
3. Compute $\mathbf{z} = G(\mathbf{y}) \in \{0,1\}^{2\ell}$.
4. Output $(\mathbf{x}, \mathbf{z}) \in \{0,1\}^{3\ell}$.

Proposition 2.4. If G is a PRNG, then H, constructed as described above, is also a PRNG.

We have already seen some bad PRNGs, so what about the good ones? Although there exist some proposals of PRNGs that are believed to be secure and are built "from scratch", what happens in practice is that, when one wants a PRNG, it is common to build it from a block cipher, which is a topic that we will cover later in the course, so we delay the examples of cryptographic PRNGs until then. For completeness, we next look at a function that is enough for most applications of pseudorandom generation, but is not secure for cryptographic use.

2.3 Linear feedback shift registers

A *linear feedback shift register* is a type of "stretching function" that produces an output that looks quite random, and it passes some statistical tests, although it is still weak from a cryptographic point of view. We will start with a particular example. Assume that we have a seed k, written as a bitstring $\mathsf{k} = k_1 k_2 k_3$. The

[2] We set the output length to be 2ℓ for simplicity, but the idea could easily be adapted to any other output length.

linear feedback shift register recursively produces each new element of the key according to the formula:

$$k_{i+3} = k_{i+1} \oplus k_i.$$

For example, if the seed is 011, the key stream will be

$$0111001 \quad 0111001 \quad 0111001 \quad 0111001 \quad 0111001 \quad \dots$$

We included the spaces to emphasize the fact that, after a while, the output seems to repeat. This is not something specific to this example, but actually happens to any linear feedback shift register.

Indeed, let us define a general *linear feedback shift register (LFSR) of length* ℓ. It starts with a seed k, expressed as a bitstring

$$\mathsf{k} = k_1 k_2 \dots k_\ell,$$

and derives each new element of the key stream according to the following: for

$$i > \ell$$

:

$$k_i = p_1 k_{i-1} \oplus \dots \oplus p_\ell k_{i-\ell},$$

for some coefficients $p_j \in \{0, 1\}$, for $j = 1, \dots, \ell$.

Proposition 2.5. The output of an LFSR of length ℓ repeats periodically, with a period of at most $2^\ell - 1$.

Note the "at most" in the statement. For some choices of the coefficients p_j, the period could be much shorter. However, for well-chosen coefficients, we can meet the bound, thus obtaining a period that is exponential in the length of the initial key. The output of a well-chosen LFSR has some good statistical properties. In particular, the output looks "random enough" for most applications. However, there are attacks that allow an adversary to distinguish the output from uniformly random, and thus LFSRs are not suited for cryptography.

Still, a clever combination of a few LFSRs, with a couple of extra details, seems to be enough to realize the stream cipher Trivium, which, to this date, is believed to be secure.[3]

Below is a direct implementation of an LFSR. You can try different sets of feedback coeffients, and see how this impacts the period of the key stream.

```
# Define the XOR operation:
def xor(a,b):
    return mod(int(a)+int(b),2)
```

[3] De Canniere, C., & Preneel, B. (2008). Trivium. In *New stream cipher designs* (pp. 244-266). Springer, Berlin, Heidelberg.

```
# Set a vector of feedback coefficients [p_1, ... , p_n]
feedback_coeffs = [1, 1, 0, 0, 0, 0, 0, 0]
seed_length = len(feedback_coeffs)

# Sample a uniformly random seed of the same length.
seed = list(random_vector(GF(2),seed_length))
print(seed)

# Choose the length of the required key stream
k = 16

# Run the LFSR
key_stream=seed
for i in range(seed_length,seed_length+k):
    key_stream_temp=0
    for j in range(seed_length):
        key_stream_temp = xor(key_stream_temp,(feedback_coeffs[j]*key_stream[i-j-1]))
    key_stream.append(key_stream_temp)
print(key_stream)
```

2.4 True randomness

We have dealt with the problem of stretching a tiny bit of randomness into something usable. But where does this initial randomness come from? It cannot really come from our computers, since these are deterministic, so the answer lies out in the physical world.[4] The general idea is to look for unpredictable processes from which to extract randomness. Some examples are radioactive decay, cosmic radiation, hardware processes like the least significant bit of the timestamp of a keystroke.

These processes might not produce uniformly random outputs, but from our perspective we have little to none information about their output distribution. These values are not used raw, but processed by a *random number generator (RNG)*, which refines them into what we assume to be uniformly random outputs. These can now be fed into our PRNGs to stretch them.

[4] Assuming, of course, that the universe is not completely deterministic.

Chapter 3

Block ciphers

In this section, we focus on block ciphers, which are a more popular alternative to stream ciphers. Block ciphers are interesting not only for encryption, but they also have some interesting theoretical implications, since many other cryptographic primitives (like pseudorandom generators) can be built from block ciphers. In this section, we will learn:

1. What is a block cipher, and what are the properties of a good block cipher;
2. The different modes of operation of a block cipher;
3. Two prime examples of block ciphers: DES and AES.

3.1 Overview of block ciphers

Recall that the one-time pad, and stream ciphers in general, encrypt bits one by one. In contrast, block ciphers will split our plaintext in blocks of fixed length, and encrypt each of this as a single unit.

Definition 3.1. *A* block cipher of length ℓ *is an encryption scheme that encrypts a message of fixed length* ℓ.

When encrypting an arbitrarily large message, we will split it into blocks of length ℓ and encrypt each block, using the same key, unlike in the previous section where we tried to stretch the key. Because of this, we will require a good block cipher to satisfy two new properties, that we informally describe below:

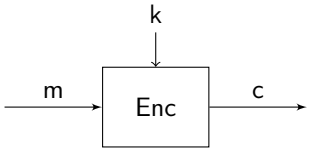
- *Confusion:* each bit of the ciphertext depends on several parts of the key. In other words, the relation between key and ciphertext must not be clear to any attacker.

- *Diffusion:* small changes in the plaintext result in significant changes in the ciphertext. More precisely, in any modern block cipher, it is expected that a single bit change in the plaintext should result in at least half of the bits of the ciphertext changing.

Later in this section, we will see some concrete examples of block ciphers used in practice. For now, let us assume that we already have some block cipher

$$(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}),$$

that we will use as a black box. That is, for now we do not know what happens inside each of the algorithms, only that they work and they are secure. For example, we assume that Enc takes as input a plaintext m of length ℓ and produces a ciphertext c corresponding to m. We represent this by the diagram



This will allow us to discuss block ciphers in a more general way.

3.2 Modes of operation

Assume that we want to encrypt a message m of length ℓn with a block cipher. When the message length is not a multiple of the block length, some extra bytes are added to complete the last block. This is called *padding*.[1] We start by splitting the message in blocks

$$\mathsf{m}_1, \ldots, \mathsf{m}_n,$$

each of them of length ℓ, so that they can be fed into our block cipher. The question is: do we encrypt each block in parallel? Is that secure? Or should we somehow make the blocks influence each other? The way we proceed here is determined by the *mode of operation* that we choose.

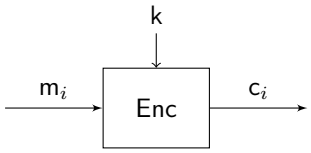
3.2.1 Electronic codebook (ECB) mode

In ECB mode, we take the most straightforward approach, and encrypt each block on its own:

$$\mathsf{c}_i = \mathsf{Enc}_k(\mathsf{m}_i).$$

The ECB mode is represented in the following diagram:

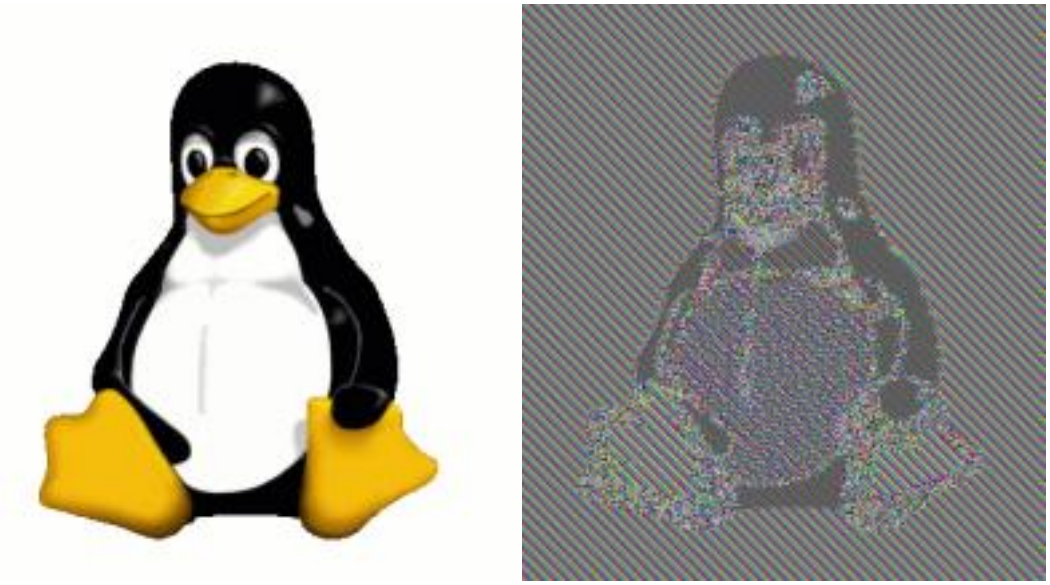
[1] One must be careful when choosing padding, as some choices are vulnerable to certain attacks in some modes of operation. An example of this is the padding oracle attack: https://en.wikipedia.org/wiki/Padding_oracle_attack.



The main advantage of this approach is that, since each block is independent, we can make the operations in parallel, potentially saving computation time.

However, this mode presents several weaknesses. For example, since each block is encrypted in exactly the same way, two identical messages result in two identical ciphertexts. So an eavesdropper can see when the same message was sent twice. Even if he does not know the content, this provides the attacker with some partial information, which is something that we would like to avoid.

Furthermore, the ECB mode is particularly bad when encrypting "meaningful" information. A very visual example comes from encrypting an image. Assume that we split the image into small squares of pixels, so that the bit length of each of these matches the length of our block cipher, and then use ECB-mode encryption on each square. Below you can see the result on an example image.[2]



Because the blocks are encrypted independently, a human eye can still easily distinguish the underlying information. This illustrates ECB mode's lack of diffusion.

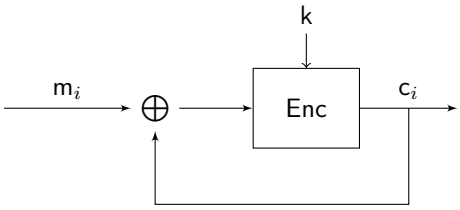
[2]Source: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation. Images by Larry Ewing (lewing@isc.tamu.edu) and GIMP (https://www.gimp.org/).

3.2.2 Cipher block chaining (CBC) mode

So we have seen that we want our blocks to interact in some way. To achieve this, the CBC mode takes the following approach: the idea is to create a *feedback loop*, in which each ciphertext produced by the block cipher is fed back into the input of the next iteration, by computing the XOR with the new input. More precisely:

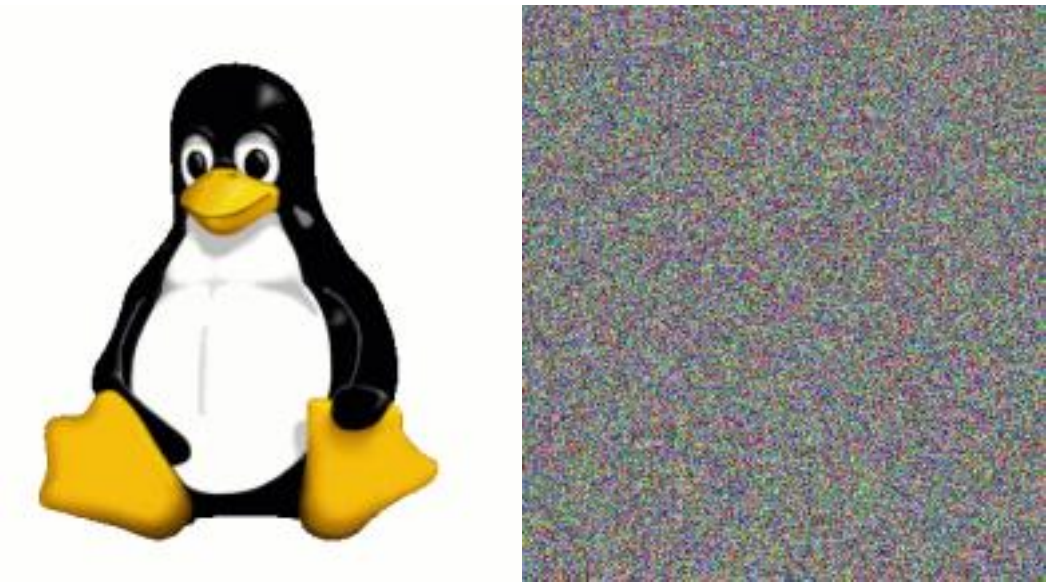
$$\mathsf{c}_i = \mathsf{Enc}_k(\mathsf{m}_i \oplus \mathsf{c}_{i-1}).$$

The CBC mode is represented in the following diagram:



Note that this does not work for the first block, since there is no previous ciphertext, and so we introduce something to replace it, which we call the *initialization vector* (often denoted by IV). By choosing the IV at random, we also introduce randomness in our scheme, making the procedure non-deterministic. Observe also that, due to the recursive nature of the definition, the encryption of a block is not only influenced by the previous block, but by *every* block that came before, and also the IV. There is no need for the IV to be secret, although it should not be reused, so if a new encryption sessions starts, a new IV should be chosen.

With this approach, we achieve a much higher diffusion. Looking again at the same picture, the result is now very different:



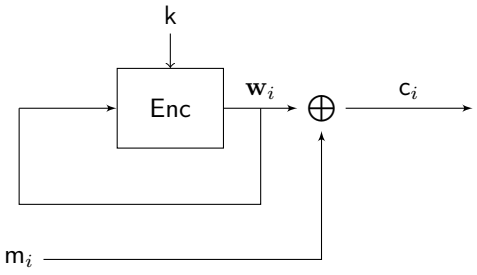
This is due to the fact that the encryption of each block influences the next. Thus, two identical blocks (for example, two squares of white in the corner of the picture) do not produce the same output anymore. The downside of this approach is that, since we need a ciphertext before we can compute the next, we cannot parallelize the computations.

3.2.3 Output feedback (OFB) mode

The next mode of operation actually turns a block cipher into a stream cipher, by recomputing a key each time through the Enc algorithm. That is, it is a stream cipher in which the key stream is produced in blocks of length ℓ:

$$\begin{aligned}\mathbf{w}_i &= \mathsf{Enc}_k(\mathbf{w}_{i-1}),\\ \mathsf{c}_i &= \mathsf{m}_i \oplus \mathbf{w}_i.\end{aligned}$$

The OFB mode is represented in the following diagram:



Again, we need an IV to feed into Enc in the first iteration. Observe that the block cipher and the feedback loop do not involve the message at all, which is simply XOR'ed with the result of each iteration of the loop to produce the ciphertext, as in any stream cipher.

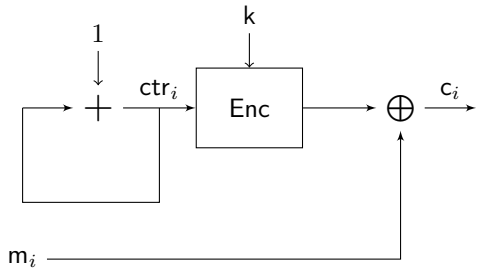
While, as the CBC mode, the computation cannot be performed in parallel, the fact that the loop does not depend on the message at all allows us to precompute a bunch of key blocks in advance, for later use with a message.

3.2.4 Counter (CTR) mode

Similarly to the OFB mode, the CTR mode produces a stream cipher from a block cipher. It works by keeping a public counter ctr that is chosen randomly, and is increased by 1 after each iteration. The counter works as an IV that updates after encrypting each block.

$$\begin{aligned} \mathsf{ctr}_i &= \mathsf{ctr}_{i-1} + 1, \\ \mathsf{c}_i &= \mathsf{m}_i \oplus \mathsf{Enc}_k(\mathsf{ctr}_i). \end{aligned}$$

After the last iteration, the current value of the counter is also sent, together with the ciphertext. The CTR mode is represented in the following diagram:



Exercise 3.1. *We have not discussed the decryption procedure of any of the modes of operation. Given a* Dec *algorithm that recovers plaintexts encrypted with* Enc*, describe how decryption works for each mode of operation. Recall that the values of the IV and counter are public.*

3.3 DES and AES

Now that we know how to use block ciphers, let us look a bit into some of the most famous ones: the *Data Encryption Standard (DES)*, and its successor the *Advanced Encryption Standard (AES)*. DES was designed by a team at IBM in 1974, and became the first official encryption standard in the US in 1977.

It remained as the recommended encryption scheme until 1999, when it was replaced by AES.[3]

3.3.1 Data Encryption Standard (DES)

DES is a block cipher of length 64, which uses a key of 56 bits. Essentially, it is composed of 16 identical rounds, each of them consisting of the following. During each round, a *round key* k_i of 48 bits is derived from the master key. In round i, the algorithm receives m_{i-1}, the output of the previous round (or the original message, for $i = 1$), and computes m_i, the output of the current round. In between, the following step happen:

1. Split m_{i-1} in two halves $\mathbf{L}_{i-1}, \mathbf{R}_{i-1}$ of 32 bits each.
2. Derive the round key k_i from k.
3. Set $\mathbf{L}_i = R_{i-1}$ and $\mathbf{R}_i = L_{i-1} \oplus f(\mathbf{R}_{i-1}, \mathsf{k}_i)$.
4. Return $\mathbf{m}_i = (\mathbf{L}_i, \mathbf{R}_i)$

After round 16, the end result m_{16} is the ciphertext.

Decryption of DES is almost the same as encryption, starting from the last round key. Observe that one half of the input of each round is not encrypted, just moved around, and so in total each half of the plaintext is encrypted 8 times by XOR'ing it with a function of the round key. There are a couple of details that we have not specified yet:

- How to derive round keys from the master key k. Without getting into much detail, the k_i is obtained from k by performing some rotations and permutations on the positions of the bits, and then some bits are ignored.
- How the function f works. First, the function expands the 32-bit input $\mathbf{R}_{i-1}$ to a 48-bit string, by repeating some of the bits in specified positions. The result is then XOR'ed with the round key k_i. The result from this operation is then split into 8 blocks of 6 bits each, and fed into what is known as *substitution boxes (S-boxes)*, which are functions specified by a lookup table. Each box outputs a string of 4 bits, so in total we have a string of 32 bits. Finally, the positions of the bits in this string are permuted, and the result is the output of the function f.

[3] Some interesting bits of history around DES and NSA involvement can be found in Chapter 3 of Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009..

The design of the cipher, specially the function f, might look arcane. Indeed, since the design and standardization of DES was not a public process, the reason behind some design choices is still not completely clear. What is known, however, is that the f function and the S-boxes were designed to thwart any attack known at the time (and even some that were not known to the public). The takeaway message here is that the S-boxes and the final permutation play a big role in achieving a good level of diffusion, propagating change through the whole ciphertext in the following rounds. Indeed, we have the following result.

Proposition 3.1. By the end of the fifth round of DES, every single bit of the current ciphertext depends on all the bits of the plaintext and all the bits of the key.

No sophisticated efficient attacks are known against DES to date. However, the key size is simply too small for today's standards (look again at the table at the end of section 1), and so it was eventually replaced by AES. Some variants of DES, like 3DES, which essentially means applying DES three times in a row, are still in use, and have withstood any attacks so far.

3.3.2 Advanced Encryption Standard (AES)

AES is a block cipher with block length 128 bits. Unlike DES, which used 56-bit keys, AES supports keys of bit length 128, 192 and 256, and has between 10 and 14 rounds, depending on the key length. Moreover, while in DES only half of the block was encrypted in each round, the full block is encrypted in every round now. On a very high level, each round consists of the following steps, called *layers*:

1. *Key addition layer:* a round key of length 128 is derived from the master key, in a process called *key schedule*.
2. *Byte substitution layer:* similarly to DES, AES uses 16 S-boxes defined by lookup tables, replacing each byte of the message by a new byte specified by the corresponding S-box. This layer introduces confusion.
3. *Diffusion layer:* the position of the bytes are permuted. Then, blocks of four bytes are combined using some matrix operations.

Regarding security, no attack more efficient than brute force is known to date. Thus, the security level provided by AES is λ, where $\lambda \in \{128, 192, 256\}$ is the bit size of the key.

The following video has a very clear and concise overview of the inner workings of AES.

Chapter 4

Hash functions

In this section, we take a detour from encryption to look at other cryptographic primitives. You might have encountered hash functions before, in a different field. However, we will see that hash functions in cryptography require some special properties. We will:

1. Briefly discuss some issues in cryptocurrencies, and how they can be solved with hash functions.
2. Define hash functions and their main properties.
3. Learn about the birthday paradox attack on hash functions.
4. Learn how to extend the domain of a hash function through the Merkle-Damgärd transformation.

4.1 Some issues in cryptocurrencies

Traditional currency is centralized, which means that there is an authority that dictates money policy, establishes ownership, and manages the whole system. On the other hand, in recent decades there has been a substantial effort in using cryptographic tools to build what we know as *cryptocurrencies*, which aim to be completely decentralized.

In this section, we discuss some issues that arise in decentralized systems. This is a very high level overview, based on the Bitcoin[1] approach, and omits many technicalities for the sake of the exposition. Nevertheless, it will be enough to motivate the use of hash functions.

[1] https://bitcoin.org/bitcoin.pdf.

A *coin*, the monetary unit of a cryptocurrency, is nothing more than a unique bitstring ID that identifies is, and is accordingly called its *identifier*. An immediate problem arises regarding transferring ownership of a coin.

Problem 1 (Double-spending). *Suppose that A buys something from B on the internet and pays with a coin ID. What prevents A from using the same coin ID to buy something else from a different party C?*

On very general terms, the solution is to publish every transaction that happens, so that the journey of each coin can be traced and thus its ownership can be established. In the problem above this means that, when A buys from B, the message "A transfers the coin ID to B" is added to the *public ledger*. Then, after the ledger awards B ownership of the coin, they can send whatever A bought. Moreover, if A tries to spend the same coin again, C will notice in the ledger that the coin no longer belongs to A, and the transaction will be denied. So, ignoring the logistics of checking and storing and increasingly large ledger, we would have solved the issue. But we still have to deal with the following problem.

Problem 2. *Who keeps track of this public ledger? Who adds the new transactions? If there is no central authority, how do users agree on which transactions happened?*

More concretely, imagine that there is a ledger of transactions

$$t_1, t_2, \ldots, t_n,$$

and two different options t_{n+1}, t'_{n+1} are claimed to be the next transaction by different parties:

$$t_1, t_2, \ldots, t_n \begin{cases} \nearrow t_{n+1} \\ \searrow t'_{n+1} \end{cases}$$

This situation is called a *fork*. The system is designed in such a way that users are encouraged to keep a *consensus* on a ledger of valid transactions. The general idea is that you have more of a say if you have more computational power, or more precisely if you have spent more CPU cycles in adding transactions to the ledger. So we need a way to "prove" that you have spent these cycles.

Let

$$H : \{0,1\}^k \to \{0,1\}^\ell,$$

for some $k, \ell \in \mathbb{N}$, where in general k is much larger than ℓ, be an efficiently computable function. Suppose that we are interested in the problem of finding $\mathbf{x}$ such that $H(\mathbf{x}) = \mathbf{0}$, where $\mathbf{0}$ is the string of zeros of length ℓ. If we know nothing about H, the best we can do is try random inputs until we find a good

one. On average, it would require 2^ℓ attempts to find such $\mathbf{x}$. That is, whoever shows a solution $\mathbf{x}$ has "proven" that he spent $O(2^\ell)$ evaluations of H in solving the problem. This concept is known as a *proof of work*.

But back to transactions and the ledger: assume that the transaction t_{n+1}, involving coin ID, is to be added to the ledger. Then, our proof of work consists of producing $\mathbf{x}$ such that the first T bits of $H(ID|\mathbf{x})$ are 0, for some T. Once you have the solution, you can add the transaction, including ID and $\mathbf{x}$, to the ledger. Note that solving the problem takes time $O(2^T)$, whereas checking a solution is efficient, as it amounts to evaluating the function H just once with the transaction as input.

But isn't this a lot of trouble to get someone's transaction up in the ledger? The solution here is extremely simple: motivate the users of the network by awarding them newly mint coins when they successfully add a new transaction to the ledger. These users are the so-called *miners*, and the act of mining a cryptocurrency is just finding the right preimages of the function H.

Thus, each addition to the ledger has two outcomes: transferring ownership of existing money and minting new money. And here's the catch: as a miner, your new money is just valid a hundred transactions after your contribution to the ledger. Give a fork, honest users are encouraged to look at the longest ledger and ignore the rest. This encourages miners to work on the single longest ledger too, because the alternatives will be rejected by the users and thus the transactions in them virtually never happened. Therefore, miners might spend CPU cycles for nothing if they decide to work on shorter ledgers of a fork.

Another issue is that we want each new transaction to be "bound" to the previous ones. If the new transaction did not depend on the previous, nothing would prevent a malicious user from double-spending. This is also achieved through the function H. Given previous transactions $t_1, \ldots, t_n$, the new transaction t_{n+1} will include its own *transaction identifier* $H(t_1, \ldots, t_n)$ besides ID and $\mathbf{x}$. However, the ledger gets larger and larger, and we want the identifier to be small to keep things efficient. So H is mapping a very large set into a smaller one. The upshot is that there is no way for transaction identifiers to be unique.

Problem 3. *What if there are two sets of transactions $t_1, \ldots, t_n$ and $t'_1, \ldots, t'_n$ with the same identifier $H(t_1, \ldots, t_n) = H(t'_1, \ldots, t'_n)$?*

Fortunately, although it is clear that there is no possible function H such that the outputs are unique, it will be enough if it is *hard* to find a pair of inputs with the same output, so that this issue with the identifiers cannot be exploited in practice.

4.2 Hash functions

The central piece of this whole apparatus seems to be the function H, which we have not looked into yet. Clearly we will require some unconventional properties

from this function. Let us summarize what we discussed about it:

- The input is larger than the output, possibly by much.
- Given $\mathbf{y}$, it should be hard to find $\mathbf{x}$ such that $H(\mathbf{x}) = \mathbf{y}$.
- It is hard to find $\mathbf{x}, \mathbf{x}'$ such that $\mathbf{x} \neq \mathbf{x}'$ and $H(\mathbf{x}) = H(\mathbf{x}')$.

With this intuition in mind, let us introduce the solution to all of our problems: *hash functions*. At their core, hash functions are nothing more than functions that take an arbitrarily-long bitstring and output a bitstring of fixed length.

Definition 4.1. *A* hash function *is an efficiently computable*[2] *function*

$$H : \{0,1\}^* \to \{0,1\}^\ell,$$

for some $\ell \in \mathbb{N}$, and where $\{0,1\}^*$ denotes the set of all bitstrings of any length. The process of computing a hash function is often called hashing*, and the output is referred to as the* hash.

Note that, unlike encryption, hash functions do not use any secret key. From a functionality point of view, this is all we need: a function that compresses bitstrings and is efficient enough to compute. However, to ensure the security of the cryptocurrency model described above, we will need an extra property.

We observe that hash functions must be public and deterministic, because different parties need to be able to arrive to the same result to verify a transaction.

The hash function is taking arbitrarily-large messages and producing fixed-length ones. That it, it is mapping a larger set into a smaller set. Therefore, there must be different strings that produce the same hash. Given a bitstring $\mathbf{b}$, there might exist $\mathbf{b}' \neq \mathbf{b}$ such that

$$H(\mathbf{b}) = H(\mathbf{b}').$$

Nevertheless, we want this pair of bitstrings to be hard to find. This, and the observations at the beginning of Section 4.2, motivate the following set of definitions.

Definition 4.2. *Let H be a hash function. We say that H is:*

- collision-resistant *if it is hard to find two bitstrings $\mathbf{b}, \mathbf{b}'$ such that $\mathbf{b} \neq \mathbf{b}'$ and $H(\mathbf{b}) = H(\mathbf{b}')$. In this case, the pair $(\mathbf{b}, \mathbf{b}')$ is called a* collision *of H.*

[2] *You might wonder what "efficiently computable" means in this case, if the input size could be anything. To be precise, we say that the function is efficiently computable if it can be evaluated in time polynomial in ℓ when the input is of length polynomial in ℓ.*

- second preimage-resistant *if, given* $\mathbf{b}$*, it is hard to find* $\mathbf{b}' \neq \mathbf{b}$ *such that they form a collision.*
- preimage-resistant *if, given* h *sampled uniformly at random, it is hard to find a bitstring* $\mathbf{b}$ *such that* $H(\mathbf{b}) = h$*.*

These properties are related by the following result.

Proposition 4.1. Let H be a hash function

$$H : \{0,1\}^* \to \{0,1\}^\ell.$$

If H is collision-resistant, then it is second preimage-resistant.

Exercise 4.1. *Try to prove the proposition above by proving the contrapositive: assume that you can break second preimage resistance, and show how to use that to break collision resistance.*

Informally, second-preimage resistance implies preimage resistance for any hash function that performs some "meaningful" compression of the input. This means that, for any hash function used in practice, if it is second-preimage resistant then it its preimage resistant, although the statement cannot be formally proven, due to some pathological counterexamples.

4.3 Birthday attacks

Assume that we are an adversary trying to attack a hash function

$$H : \{0,1\}^* \to \{0,1\}^\ell,$$

that is, we are trying to find a collision. The straightforward approach is the following: we choose random strings and compute their hashes, until two strings return the same hash. In the worst case, this requires $2^\ell + 1$ tries, since there are at most 2^ℓ different outputs. Therefore, it looks like the brute-force attack takes time $O(2^\ell)$ to succeed. This would suggest that a hash function with output length ℓ gives us a security level of ℓ.

In this section, we look into a generic attack that works for any hash function, which is based on the well-known *birthday paradox* from probability theory, and greatly improves over the above estimation. Consider the following problem.

Problem 4. *There is a room with* 40 *independent students. How likely is that any two of them share the same birthday?*

On first sight, one might think that this probability is quite low. After all, there are 356 days in the year, and only 40 students. Let us compute the actual probability, by solving a related problem: what is the probability of none of the 40 students sharing their birthday?

We start by numbering the students from 1 to 40, according to any criterion. To be able to reason more formally about the problem, we introduce the function

$$\mathsf{bd} : \{1, \ldots, 40\} \to \{1, \ldots, 365\},$$

which associates to each student its birthday. Then, the probability of student #2 not sharing a birthday with student #1 is

$$\Pr[\mathsf{bd}(1), \mathsf{bd}(2) \text{ are different}] = \frac{364}{365},$$

since there are 364 days of the year that are not the birthday of student #1. Let's introduce student #3 into the picture, and let us consider the events:

- A: $\mathsf{bd}(3)$ is different from $\mathsf{bd}(1)$ and $\mathsf{bd}(2)$.
- $\mathsf{B} : \mathsf{bd}(1), \mathsf{bd}(2)$ are different.

Clearly, the intersection event is

- $\mathsf{A} \cap \mathsf{B} : \mathsf{bd}(1), \mathsf{bd}(2), \mathsf{bd}(3)$ are pairwise different.

Then, using conditional probabilities, we have that

$$\Pr[\mathsf{A} \cap \mathsf{B}] = \Pr[\mathsf{B}] \cdot \Pr[\mathsf{A}|\mathsf{B}]$$

We already know $\Pr[\mathsf{B}]$, so we are just missing the second term. If the birthdays of students #1 and #2 are different, then the probability of #3 having a different birthday from them is

$$\Pr[\mathsf{A}|\mathsf{B}] = \frac{363}{365},$$

since there are 363 days that are neither the birthday of #1 or #2. Thus, the probability of the three students having different birthdays is

$$\Pr[\mathsf{A} \cap \mathsf{B}] = \frac{364}{365} \cdot \frac{363}{365}.$$

By iterating this process for each student, we arrive at the conclusion that the probabilities of all 40 students having different birthdays is

$$\frac{364}{365} \cdot \frac{363}{365} \cdot \cdots \cdot \frac{326}{365} \approx 0.108768.$$

In conclusion, the probability of two students sharing a birthday is approximately

$$1 - 0.108768 = 0.891232.$$

This is actually a pretty high probability. This discrepancy between what one might naively expect and what actually happens is known as the *birthday paradox*. Below, you can find the solutions to Problem 4 for different numbers of students (rounded to six decimal positions).

Students	Probability
10	0.116948
20	0.411438
40	0.891232
80	0.999914
128	0.999999

So what does any of this have to do with breaking a hash function? What we have just done is computing the probability of finding two students such that the birthday function returns the same value on them. That is, we have found a collision of the birthday function! In doing so, we have assumed that the output of the birthday function behaves as the uniform distribution on $\{1, \ldots, 365\}$. But, isn't that exactly the effect that we want from a good hash function? That outputs look random and unrelated? So the moral of the story is that finding collisions in a hash function is actually much more likely that expected. More precisely, it can be proven with some careful probabilities analysis that, for any hash function H which outputs bitstrings of length ℓ, there is a decent probability of finding a collision after $\sqrt{2^\ell}$ evaluations.

Compare this with our initial estimation. At the beginning of the section, we bounded a brute force attack by $O(2^\ell)$. However, we now see that an attacker has a good probability of finding a collision in time $O(2^{\frac{\ell}{2}})$. Thus, we conclude that a hash function with output length ℓ gives us $\ell/2$ bits of security. Or the other way around, if we want ℓ bits of security, we need our hash function to have output length 2ℓ.

4.4 The Merkle-Damgård transformation

As was the case for encryption, we often build hash functions in two steps. First, we build a hash function for fixed-length inputs, e.g.

$$H : \{0,1\}^{2\ell} \to \{0,1\}^\ell,$$

and then we extend them to arbitrarily-large input. We will not get into the details of concrete constructions, but will simply mention the SHA family of hash functions, which is the standard used in practice most of the time.[3]

A common way to realize this second step is to use the *Merkle-Damgård transformation*,[4] which describes how to build from H another hash function $\mathbf{H}$ that

[3] https://en.wikipedia.org/wiki/Secure_Hash_Algorithms.

[4] You might also see the same concept named the Merkle-Damgård transform, or the Merkle-Damgård construction.

takes as input any string of length at most $2^\ell - 1$, and outputs a hash of length ℓ. It is clear that repeated applications of the transformation can make the input go as large as we want.

Similar to modes of operations in block ciphers, the Merkle-Damgård transformation starts by splitting the string $\mathbf{x}$ of length $L \leq 2^\ell$ to be hashed into blocks

$$\mathbf{x}_1, \ldots, \mathbf{x}_n,$$

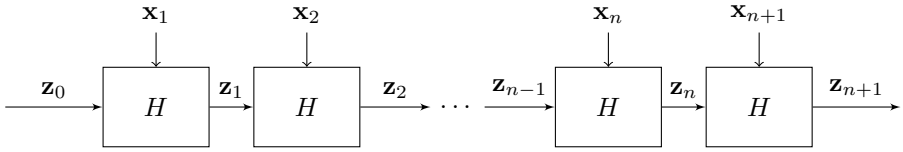
each of them of length ℓ.[5] An additional block $\mathbf{x}_{n+1}$ is added, containing a binary encoding of L. Note that, because $L \leq 2^n - 1$, we can fit the encoding of L in n bits. Then, we recursively compute

$$\mathbf{z}_i = H(\mathbf{z}_{i-1}|\mathbf{x}_i),$$

for $i = 1, \ldots, n+1$, and where $(\mathbf{z}_{i-1}|\mathbf{x}_i)$ means the concatenation of the bitstrings $\mathbf{z}_{i-1}$ and $\mathbf{x}_i$. Then, the hash of $\mathbf{x}$ is

$$\mathbf{H}(\mathbf{x}) = \mathbf{z}_{n+1}.$$

As in modes of operation, there is no "previous block" in the first iteration, and so again we introduce an initialization vector $\mathbf{z}_0$, which can be set to the string of 0's of length n, or any other bitstring. There is no need for the IV to be secret.



Proposition 4.2. If H is a collision-resistant hash function, then $\mathbf{H}$, produced with the Merkle-Damgård transformation, as described above, is also collision-resistant.

[5] As before, use some padding if the length of $\mathbf{x}$ is not a multiple of ℓ.

Part III

Asymmetric cryptography

Chapter 5

Elementary number theory

The second half of the course relies strongly on some ideas from number theory, which is the branch of mathematics that deals with integer numbers and their properties. This section and the next contain mathematical background that we will require to build some asymmetric cryptography. In this section, we will:

1. Review integer and modular arithmetic.
2. Discuss algorithmic aspects of modular arithmetic.

Note. In these notes, we use the convention that $\mathbb{N}$ does not include 0. We will refer to the set of non-negative integers by $\mathbb{Z}_{\geq 0}$.

5.1 Integer arithmetic

Consider the set $\mathbb{Z}$ of integer numbers. A key concept to the whole section is that of *divisibility*.

Definition 5.1. *Let $a, b \in \mathbb{Z}$. We say that b* divides *a if there exists $m \in \mathbb{Z}$ such that*

$$bm = a.$$

We denote that b divides a by $b \mid a$. In this case, we also say that b is a divisor *or* factor *of a, or that a is* divisible *by b, or that a is a* multiple *of b.*

Note that it is crucial that $m \in \mathbb{Z}$ in the definition above. Otherwise, any number b would divide any other number a, since

$$b\frac{a}{b} = a,$$

and then this notion would be pretty meaningless. Divisibility is related to the notion of *integer division*.

Proposition 5.1 (Integer division)**.** Let $a, b \in \mathbb{Z}$, with $b \neq 0$. Then, there exists a unique pair $q, r \in \mathbb{Z}$ such that $0 \leq r < b$ and

$$a = bq + r.$$

The integer q is called the *quotient* of the division, and r is called the *remainder.*

In Sage, quotient and remainder can easily be computed with the commands `a // b` and `a % b`, (or `mod(a,b)`) respectively.

By looking at the above proposition and the definition of divisibility, it is easy to see that $a \mid b$ if and only if the remainder of the division of a by b is 0.

Divisibility allows us to identify a special type of integers that are the building blocks of any other integer number. Clearly, any integer $n \in \mathbb{Z}$ is always divisible by $1, -1, n$ and $-n$, which are called its *trivial divisors.* Some numbers have more divisors, and some do not.

Definition 5.2. *An integer $p > 1$ is said to be a* prime number *if its only divisors are the trivial divisors. A positive integer that is not prime is said to be* composite.

Exercise 5.1. *Decide whether each of these statements is true or false:*

1. 35 *is a divisor of* 7.
2. 4 *is a factor of* 16.
3. 99 *is divisible by* 9.
4. *The remainder of dividing* -21 *by* 8 *is* -5.
5. 19 *is a prime number.*
6. 41 *is a composite number.*

The following two results show some interesting properties of prime numbers. Informally, the first states that any number can be decomposed into its prime factors, and that this decomposition is essentially unique, and the second states that, asymptotically, the chance of choosing a random number smaller than n and finding a prime is $\log(n)/n$.

Proposition 5.2 (Fundamental theorem of arithmetic)**.** Let $n \in \mathbb{Z}$. Then there exist prime numbers $p_1, \ldots, p_\ell$ and integers $e_1, \ldots, e_\ell$ such that

$$n = \pm p_1^{e_1} \ldots p_\ell^{e_\ell}.$$

Moreover, this *decomposition* (or *factorization*) is unique, up to reordering of the factors.

Proposition 5.3 (Prime number theorem)**.** Let $n \in \mathbb{N}$, and let us denote by $\pi(n)$ the number of prime numbers smaller than n. Then

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\log(n)} = 1.$$

On a computational level, one might think that the problem of determining whether a number is prime or composite and the problem of finding the factorization of said number are close problems. However, the surprising truth is that the second is believed to be much harder than the first! More precisely, there exist efficient algorithms for determining whether a number is prime, but no efficient factorization algorithm is known for numbers that are a product of two large primes, despite decades of huge efforts in finding one.[1]

Sage contains implementations of the best algorithms known for each case. Try increasing the size of the numbers, and observe that the first algorithm is still very fast, but factorization becomes much slower.

```
from sage.misc.prandom import randrange

# Choose a security parameter, which will determine the size of our numbers.
sec_param = 160

### Primality testing
# Pick a random number of bitlength sec_param
n = randrange(2^(sec_param-1),2^(sec_param))
# Run a primality test
%time print(n in Primes())              # Sage contains the class Primes().
                                        # By checking whether n is in Primes(),
                                        # it is actually running a primality test internally.

### Factorization
# Pick two primes of bitlength half of sec_param.
# This is so that their product has bitlength sec_param.
p = random_prime(2^((sec_param/2)-1),2^(sec_param/2))
q = random_prime(2^((sec_param/2)-1),2^(sec_param/2))
# Compute their product
n = p*q
%time print(factor(n))
```

[1] For those with a background in complexity theory, primality is a problem in P and factorization is a problem in NP.

5.2 The euclidean algorithm

With Proposition 5.2 in mind, we observe that two integers a, b can have some factors in common in its prime factorization. This gives rise to the following notion.

Definition 5.3. *Let $a, b \in \mathbb{Z}$ different from 0. The* greatest common divisor *of a and b, denoted by*

$$\gcd(a, b),$$

is the largest positive integer k such that $k \mid a$ and $k \mid b$. Two integers a, b are said to be coprime *(or* relatively prime*) when*

$$\gcd(a, b) = 1.$$

Think about the relation between the notions of primality and coprimality. In particular, observe that being prime is a property of a single integer, whereas being coprime refers to a *pair* of integers.

Exercise 5.2. *Find a pair $a, b \in \mathbb{Z}$ for each of the following cells in this table:*

	a, b prime	*a prime, b composite*	*a, b composite*
a, b coprime			
a, b not coprime			

Computing the greatest common divisor of two integers can be achieved easily using the *Euclidean algorithm*, which we describe next. Let $a, b \in \mathbb{Z}$ different from 0. The following procedure outputs $\gcd(a, b)$:

1. Compute the integer division of a by b, obtaining q, r such that $0 \leq r < b$ and
$$a = bq + r.$$
2. If $r = 0$, then output b. Otherwise, return to the previous step, replacing a by b and b by r.

We show an example for the numbers 375 and 99. We start by performing the integer division of 375 by 99, obtaining

$$375 = 99 \cdot 3 + 78.$$

Since the remainder is not 0, we compute the integer division of 99 by 78, obtaining

$$99 = 78 \cdot 1 + 21.$$

We continue with this process until the remainder is 0:

$$78 = 21 \cdot 3 + 15.$$
$$21 = 15 \cdot 1 + 6.$$
$$15 = 6 \cdot 2 + 3.$$
$$6 = 3 \cdot 2 + 0.$$

Since the remainder is 0, the Euclidean algorithm outputs $\gcd(375, 99) = 3$.

The greatest common divisor satisfies the following property.

Proposition 5.4. Let $a, b \in \mathbb{Z}$ different from 0. There exist $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b).$$

It turns out that we can slightly tweak the Euclidean algorithm to compute the integers x, y in the proposition above. This is called the *extended Euclidean algorithm*. The key idea is to use the Euclidean algorithm to compute the greatest common divisor, and then "walk back" through the computations. We illustrate it with the example of 375 and 99 from above.

We got the sequence of remainders $78, 21, 15, 6, 3, 0$, so the last one before 0, in this case 3, was our greatest common divisor. We proceed by arranging the relations between them obtained above to write each in terms of the previous two. We start with

$$3 = 15 - 6 \cdot 2.$$

We now write 6 in terms of the two previous remainders, 15 and 21:

$$6 = 21 - 15 \cdot 1.$$

Combining these two expressions, we can obtain an expression of 3 in terms of 15 and 21:

$$3 = 15 - (21 - 15 \cdot 1) \cdot 2 = -21 \cdot 2 + 15 \cdot 3.$$

Iterating this process, we can work our way back through the sequence of remainders, until we arrive at the beginning, that is, an expression depending only on 375 and 99:

$$\begin{aligned} 3 &= -21 \cdot 2 + 15 \cdot 3 = -21 \cdot 2 + (78 - 21 \cdot 3) \cdot 3 = \\ &= 78 \cdot 3 - 21 \cdot 11 = 78 \cdot 3 - (99 - 78) \cdot 11 = \\ &= -99 \cdot 11 + 78 \cdot 14 = -99 \cdot 11 + (375 - 99 \cdot 3) \cdot 14 = \\ &= 375 \cdot 14 + 99 \cdot (-53). \end{aligned}$$

Thus, we have found that

$$3 = 375 \cdot 14 + 99 \cdot (-53).$$

From a computational point of view, both versions of the Euclidean algorithm are very efficient, even for large numbers, as you can check with the following Sage code.

```
from sage.misc.prandom import randrange

# Choose a security parameter, which will determine the size of our numbers.
sec_param = 128

# Choose a pair of integers of bitlength sec_param
a = randrange(2^(sec_param-1),2^(sec_param))
b = randrange(2^(sec_param-1),2^(sec_param))

# Euclidean algorithm
%time print(gcd(a,b))

# Extended euclidean algorithm. The three outputs correspond
# to gcd(a,b), and the two numbers x,y such that gcd(a,b)=ax+by.
%time print(xgcd(a,b))
```

5.3 Modular arithmetic

Modular arithmetic is, informally, clock arithmetic. Let us take the usual analog 12-hour clock, and say it is 11 o'clock now. After three hours, it is 2 o'clock. But wait a minute, shouldn't it be $11+3=14$? Furthermore, after a whole day, shouldn't the clock show $11+24=35$ o'clock? But it is showing 11 instead!

This example shows that the usual integer arithmetic is not useful for modelling the behaviour of a clock. Let us see how we can modify it so that the passing of time makes sense again. We consider the following problem.

Let $a \in \mathbb{N}$. Assume that the current position of the clock is 12 o'clock. What is the position of the clock after a hours?

The key observation is that full movements around the clock (that is, multiples of 12) do not matter, as they leave the clock in the same position. Recall that the algorithm of integer division tells us how to compute $q, r \in \mathbb{Z}$ such that

$$a = 12 \cdot q + r.$$

In the context of our problem, notice that q is the number of full circles around the clock that happen in a hours. Then, the only real change of position in the clock is determined by r, and q does not matter at all.[2]

Generalizing this idea leads to the key concept of modular arithmetic, by replacing 12 by any positive integer. Moreover, observe that there is no need for a to be a positive integer, as a negative value of a can be interpreted as moving counter-clockwise.

[2]The only small caveat is that, when a is a multiple of 12, the remainder will be 0, not 12, although both of these represent the same position. So, to be precise, let us assume that our clock has a 0 instead of 12, so that it perfectly aligns with the remainders.

Definition 5.4. *Let $a, n \in \mathbb{Z}$, with $n > 0$. We define the* remainder *(or* residue*) of a modulo n as the remainder of the integer division of a by n, and we denote it by*

$$a \bmod n.$$

Exercise 5.3. *Compute the following values:*

$$25 \bmod 8, \qquad 1337 \bmod 7, \qquad 7 \bmod 13, \qquad -13 \bmod 12.$$

Modular arithmetic behaves in a similar way to usual arithmetic, as reflected in the following result:

Proposition 5.5. Let $a, b, n \in \mathbb{Z}$, with $n > 0$. Then:

$$\begin{array}{ll} (i) & (a \bmod n) + (b \bmod n) = (a + b) \bmod n. \\ (ii) & (a \bmod n) \cdot (b \bmod n) = (a \cdot b) \bmod n. \\ (iii) & \text{If } b \geq 0, \text{ then } (a \bmod n)^b = (a^b) \bmod n. \end{array}$$

It is clear that, when working modulo n, for some positive integer n, the only numbers that matter are $0, 1, \ldots, n-1$, since every other number can be identified with one of these by reducing modulo n. For example, back to the clock example, we have that $13 \bmod 12 = 1$, $25 \bmod 12 = 1$, and so on. It is not chance that related numbers are precisely those that represent the same position!

The above example seems to suggest that, modulo 12, the numbers

$$\ldots -23, -11, 1, 13, 25 \ldots$$

are "the same". This motivates the introduction of the idea of *congruence*.

Definition 5.5. *Let $a, b, n \in \mathbb{Z}$, with $n > 0$. We say that a and b are* congruent *if*

$$(a - b) \bmod n = 0.$$

In this case, we represent this fact by

$$a \equiv b \pmod{n}.$$

We define the set of residue classes modulo n *as the set*

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\},$$

where the operations of addition and multiplication are reduced modulo n, according to Proposition 5.5.

Then, the above discussion can be rephrased as follows. We can say that any $a \in \mathbb{Z}$ is congruent to its residue modulo n, that is, $a \bmod n$. Thus, to work with arithmetic modulo n, we can restrict ourselves to the set $\mathbb{Z}_n$.

Proposition 5.6. Let $a, \alpha, b, n \in \mathbb{Z}$, with $n > 0$. If $a \equiv \alpha \pmod{n}$, then:

$$\begin{array}{ll} (i) & a + b \equiv \alpha + b \pmod{n}. \\ (ii) & a \cdot b \equiv \alpha \cdot b \pmod{n}. \\ (iii) & \textit{If } b \geq 0, \textit{ then } a^b \equiv \alpha^b \pmod{n}. \end{array}$$

In particular, this is true when $\alpha = a \bmod n$.

Exercise 5.4. *Prove that the logic* XOR *operation and addition modulo* 2 *are the same operation, by checking the four possible cases.*

We now introduce *modular inverses*. Let $a \neq 0$ be a number, and consider the meaning of b being the inverse of a. Over the real numbers, we say that the inverse of 3 is $1/3$, because

$$3 \cdot \frac{1}{3} = 1.$$

That is, every nonzero number $a \in \mathbb{R}$ has an inverse $1/a \in \mathbb{R}$. Consider now the same idea, but over $\mathbb{Z}$. That is, given $a \in \mathbb{Z}$, is there any other integer $b \in \mathbb{Z}$ such that $ab = 1$? It is clear that, unless $a = \pm 1$, there is no such thing as an "integer inverse". However, the answer changes when we consider $\mathbb{Z}_n$ instead of $\mathbb{Z}$.

Definition 5.6. *Let $n \in \mathbb{N}$, and $a \in \mathbb{Z}_n$. We say that $b \in \mathbb{Z}_n$ is the* inverse of a modulo n* if

$$ab \bmod n = 1.$$

If the inverse of a modulo n exists, we say that a is *invertible*. We also say that a is a *unit*.*

As an example, observe that in $\mathbb{Z}_5$ we have

$$(2 \cdot 3) \bmod 5 = 6 \bmod 5 = 1.$$

Therefore, 2 and 3 are inverses modulo 5. In $\mathbb{Z}_3$, we have

$$(2 \cdot 2) \bmod 3 = 4 \bmod 3 = 1.$$

That is, 2 is its own inverse modulo 3.

Exercise 5.5. *Consider $\mathbb{Z}_4$. Find which of its elements are invertible, and which are not.*

When working with modular residues in Sage, one nice thing is that we can specify that we are working modulo some n, and Sage will take care of the modular reductions for us, without having to specify every time that we want each operation reduced modulo n. In the example below, you can see that, when asked about $a+b$, we get 7 because the operation is automatically reduced modulo 17, since we have specified that we want our operations involving a, b to be reduced modulo n. Similarly, the inverse of a is automatically computed modulo n, otherwise we would obtain $1/11$ instead of 14.

```
n=17
G=Integers(n)
G

a = G(11)
b = G(13)
a,b
a+b
a^(-1)
```

The above examples and exercise highlight that, given some n, some elements of $\mathbb{Z}_n$ have an inverse, and some do not. This motivates the following definition.

Definition 5.7. *Let $n \in \mathbb{N}$. We denote by $\mathbb{Z}_n^*$ the subset of $\mathbb{Z}_n$ formed by all the invertible elements of $\mathbb{Z}_n$. We define the function φ that, on input n, returns the size of $\mathbb{Z}_n^*$. This function is called* Euler's totient (or phi) function.

In Sage, Euler's function on input n can be computed by `euler_phi(n)`.

Proposition 5.7. Let $n \in \mathbb{N}$. Then $\mathbb{Z}_n^*$ is composed of all the elements $a \in \mathbb{Z}_n$ such that are coprime to n.

The value of the totient function, and thus the size of $\mathbb{Z}_n^*$, is determined by the prime factorization of n. More precisely, we have the following result.

Proposition 5.8. Let $n \in \mathbb{N}$. Then:

If $n = p^e$, where p is a prime and $e \in \mathbb{N}$, we have

$$\varphi(n) = (p-1)p^{e-1}.$$

If $n = pq$, where p, q are coprime, then

$$\varphi(n) = \varphi(p)\varphi(q).$$

Exercise 5.6. *Use the result above to deduce a formula for $\varphi(n)$, when n is the product of two different prime numbers.*

To actually find the inverse of an element a modulo n, we can use the extended Euclidean algorithm. The key idea is to run the extended Euclidean algorithm on a and n. The algorithm produces $x, y \in \mathbb{Z}_n$ such that

$$ax + ny = \gcd(a, n).$$

By reducing both sides of the equation above modulo n, we get that

$$ax \equiv \gcd(a, n) \pmod{n}.$$

Due to Proposition 5.7, we know that a will be invertible modulo n if and only if $\gcd(a, n) = 1$. Thus, if this is the case, we would have

$$ax \equiv 1 \pmod{n},$$

which means that x is the inverse of a modulo n. If we find that $\gcd(a, n) \neq 1$, then a is not invertible modulo n.

We also introduce the *Chinese remainder theorem (CRT)*, which, in its simplest form, states the following.

Proposition 5.9 (Chinese remainder theorem)**.** Let $a, b \in \mathbb{N}$ be coprime, and let $n = ab$. Then, for each $x \in \mathbb{Z}_n$, there exists a unique pair $(y, z) \in \mathbb{Z}_a \times \mathbb{Z}_b$ such that

$$\begin{aligned} x &\equiv y \pmod{a}, \\ x &\equiv z \pmod{b}. \end{aligned}$$

Moreover, given $(y, z) \in \mathbb{Z}_a \times \mathbb{Z}_b$, we can explicitly recover the corresponding x by computing

$$x = \left(by \left(b^{-1} \bmod a\right) + az \left(a^{-1} \bmod b\right)\right) \bmod n.$$

With the notations of the proposition above, the Sage command that computes the value x given by the Chinese remainder theorem is `crt(y, z, a, b)`.

The legend says that this theorem was used in ancient China to count troops, proceeding as follows. Say that you had 200 troops before battle, and you want to count your losses.

1. Choose a pair of coprime numbers such that their product is at least the upper bound on the number of troops. In this case, we can use $11 \cdot 19 = 209$.
2. Order the troops to stand in columns of length 11. The last column (possibly incomplete) tells us the remainder modulo 11, say it is 8.
3. Reorganize the troops in columns of length 19. Again, the last column tells us the remainder z modulo 19, say it is 2.
4. Using the Chinese remainder theorem, we know that there is a unique number $x < 209$ such that

   $$\begin{aligned} x \bmod 11 &= 9, \\ x \bmod 19 &= 2, \end{aligned}$$

   and the second part of the theorem allows us to explicitly compute this number. Since

   $$\begin{aligned} 19^{-1} \bmod 11 &= 7, \\ 11^{-1} \bmod 19 &= 7, \end{aligned}$$

   we have that

   $$x = (11 \cdot 9 \cdot 7 + 19 \cdot 2 \cdot 7) \bmod 209 = 97.$$

Higher factors, or more than two of them, can be used to deal with larger numbers.

5.4 Modular arithmetic, but efficient

There are different approaches to actually do computations modulo n. The end result will not change, but some ways involve easier computations than others. As an example, say that we want to compute

$$3^{75} \bmod 191.$$

The straightforward approach is to compute 3^{75}, which is

$$608266787713357709119683992618861307,$$

by performing 74 multiplications by 3, and then perform the division by 191. But clearly this is a lot of work. A better approach is to perform the exponentiation in smaller increments, and reduce modulo 191 before numbers get too big. More precisely, let us write the base-2 expansion of 75:

$$75 = 2^6 + 2^3 + 2^1 + 2^0. \tag{5.1}$$

Then, we can rewrite

$$3^{75} = 3^{2^6} \cdot 3^{2^3} \cdot 3^{2^1} \cdot 3^{2^0}. \tag{5.2}$$

Now observe that, for any $i \in \mathbb{N}$, we have that

$$3^{2^i} = \left(3^{2^{i-1}}\right)^2,$$

and thus each of these terms can be recursively computed from the previous by squaring. We also perform the reductions modulo 191 at each step, to prevent the numbers from blowing-up in size. Note that this reduction can be done due to point (iii) in Proposition 5.5.

$$\begin{aligned}
3^{2^0} &\equiv 3 \pmod{191},\\
3^{2^1} &\equiv \left(3^{2^0}\right)^2 \equiv 9 \pmod{191},\\
3^{2^2} &\equiv \left(3^{2^1}\right)^2 \equiv 81 \pmod{191},\\
3^{2^3} &\equiv \left(3^{2^2}\right)^2 \equiv 6561 \equiv 67 \pmod{191},\\
3^{2^4} &\equiv \left(3^{2^3}\right)^2 \equiv (67)^2 \equiv 4489 \equiv 96 \pmod{191},\\
3^{2^5} &\equiv \left(3^{2^4}\right)^2 \equiv (96)^2 \equiv 9216 \equiv 48 \pmod{191},\\
3^{2^6} &\equiv \left(3^{2^5}\right)^2 \equiv (48)^2 \equiv 2304 \equiv 12 \pmod{191}.
\end{aligned}$$

Now it simply remains to multiply the four factors of equation (5.2). Again, to avoid big numbers, we reduce modulo 191 after each factor is multiplied:

$$\begin{aligned} 3^{2^0} \cdot 3^{2^1} &\equiv 9 \cdot 81 \equiv 729 \equiv 156 \pmod{191}, \\ \left(3^{2^0} \cdot 3^{2^1}\right) \cdot 3^{2^3} &\equiv 156 \cdot 67 \equiv 10452 \equiv 138 \pmod{191}, \\ \left(3^{2^0} \cdot 3^{2^1} \cdot 3^{2^3}\right) \cdot 3^{2^6} &\equiv 138 \cdot 12 \equiv 1656 \equiv 128. \end{aligned}$$

Therefore, we conclude that

$$3^{75} \bmod 191 = 128 \qquad \text{(or, equivalently, that } 3^{75} \equiv 128 \pmod{191}\text{)}.$$

This algorithm is known as *square-and-multiply*, and the reason behind the name is clear once we take a step back and slightly rewrite our solution. Observe that, from equation (5.1), we directly deduce that the binary expression of 75 is

$$[75]_2 = 1001010.$$

Then, from the base number, in this case 3, and for each bit in $[75]_2$, starting from the right, we

- *Squaring step:* compute the square of the previous power of 3.
- *Multiplication step:* if the bit is 1, multiply the product so far by the new power of 3. Otherwise, skip this step.

Take a moment to review the example above, and convince yourself that it matches the steps described.

Chapter 6

Algebraic structures

We complete our exposition of the mathematical background by discussing some common algebraic structures, which generalize what we have seen in the previous section. Informally, an algebraic structure is a set with one or more operations on the elements of the set. The properties of these operations determine the kind of structure that we have. In this section, we will learn about two of these:

1. Groups.
2. Finite fields.

6.1 Groups

Groups are the simplest algebraic structure that we will study, since they only have one operation.

Definition 6.1. *A* group *is a pair* $(\mathbb{G}, \circ)$*, where* $\mathbb{G}$ *is a set and* $\circ$ *is an operation on* $\mathbb{G}$*, that is, a function*

$$\begin{aligned} \circ : \ \mathbb{G} \times \mathbb{G} &\to \mathbb{G} \\ (x, y) &\mapsto x \circ y, \end{aligned}$$

which additionally satisfies the following properties:

1. Associative law: $(x \circ y) \circ z = x \circ (y \circ z)$ *for all* $x, y, z \in \mathbb{G}$.
2. Existence of identity: *there exists* $e \in \mathbb{G}$ *such that* $e \circ x = x \circ e = x$ *for all* $x \in \mathbb{G}$*. Such element* e *is called the* identity element.

3. Existence of inverse: *for any $x \in \mathbb{G}$, there exists $y \in \mathbb{G}$ such that $x \circ y = y \circ x = e$, where e is the identity element. Such y is called the* inverse *of x.*

A group is said to be commutative *(or* abelian*) if it satisfies the following additional property:*

1. Commutativity: *$x \circ y = y \circ x$ for all $x, y \in \mathbb{G}$.*

The order *of a group is the number of elements in $\mathbb{G}$, if the set is finite, and infinite otherwise, and is denoted by $ord(\mathbb{G})$.*

When there is no ambiguity about the operation, we will refer to the group $\mathbb{G}$, instead of $(\mathbb{G}, \circ)$, for simplicity. Most of the time, the group operation will be (possibly modular) addition or multiplication, although these are not the only possible cases. Let us consider some examples, and see whether they are groups or not.

- $(\mathbb{Z}_{\geq 0}, +)$, where $\mathbb{Z}_{\geq 0}$ is the set of non-negative elements of $\mathbb{Z}$, and $+$ is integer addition. Integer addition is associative, and there is an identity element 0. However, there is no $x \in \mathbb{Z}_{\geq 0}$ such that

  $$1 + x = 0,$$

  and therefore $(\mathbb{Z}_{\geq 0}, +)$ is not a group.

- $(\mathbb{Z}, +)$ is a group of infinite order, since the operation is still associative, there is an identity element 0, and for any $x \in \mathbb{Z}$, there exists $y = -x \in \mathbb{Z}$ such that

  $$x + y = y + x = 0.$$

  For similar reasons, the pair $(\mathbb{Z}_n, +)$, for $n \in \mathbb{N}$, is also a group, of order n.

- For $n \in \mathbb{N}$, the pair $(\mathbb{Z}_n^*, \cdot)$, where $\cdot$ is multiplication modulo n, is a group of order $\varphi(n)$. The operation is clearly associative, 1 is an identity element for multiplication, and every element $x \in \mathbb{Z}_n^*$ has an inverse $x^{-1} \in \mathbb{Z}_n^*$, by definition of $\mathbb{Z}_n^*$.

- The pair $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$, where $+$ means component-wise addition in their respective moduli, is a group of order 6. Indeed, it is easy to see that a product of two groups is a group.

Moreover, since the operations are commutative, all of these groups are commutative.

Exercise 6.1. *Explain why none of the following is a group:*

1. $(\mathbb{Z}, \cdot)$, *where* $\cdot$ *is integer multiplication.*

2. $(\mathbb{Z}_n, \cdot)$, *where* $\cdot$ *is multiplication modulo* n, *for* $n \in \mathbb{N}$.

Group notation. In the above examples, you can observe that the notation differs from case to case, depending on the nature of the operation. For example, given some element x, we denote its inverse with respect to addition by $-x$, and its inverse with respect to multiplication by x^{-1}. Applying the operation to n copies of the same element x is represented by nx in additive notation, and by x^n in multiplicative notation. Even though not all group operations are addition or multiplication, it is common to adopt their notation for a generic group operation.[1] In these notes, we will often use multiplicative notation for generic groups. That is, we denote the identity element by 1, the inverse of x by x^{-1}, and the operation of x and y by $x \cdot y$ or simply xy.

Observe that, if a group $\mathbb{G}$ contains an element g, then the fact that $g^2 = gg$ implies that $g^2 \in \mathbb{G}$ too. Similarly, $g^3 = g^2 g \in \mathbb{G}$, and so on. It is easy to generalize this idea, and conclude that, if $g \in \mathbb{G}$, then $g^n \in \mathbb{G}$ for all $n \in \mathbb{N}$. That is, a single element g *generates* many elements of a group. This leads us to the concept of *cyclic groups*, which are those that contain only the powers of a single element.

Definition 6.2. *A group* $\mathbb{G}$ *is said to be* cyclic *if there exists* $g \in \mathbb{G}$ *such that*

$$\mathbb{G} = \{g^n \mid n \in \mathbb{Z}_{\geq 0}\}.$$

This group is also denoted by $\langle g \rangle$, *and is called the group* generated *(or* spanned*) by* g, *and* g *is called a* generator *of* $\mathbb{G}$. *Note that, in a group with additive notation, we would write instead*

$$\mathbb{G} = \{nx \mid n \in \mathbb{Z}_{\geq 0}\}.$$

The name of these groups come from their often cyclic nature. We illustrate this with the example of the group $\mathbb{Z}_5$ with addition modulo 5. We claim that

[1] A prime example of a different group operation, which appears very often in cryptography, is the group law of elliptic curves.

$\mathbb{Z}_5$ is generated by 2. Indeed,

$$\begin{aligned}
&2 \cdot 0 \bmod 5 = 0\\
&2 \cdot 1 \bmod 5 = 2\\
&2 \cdot 2 \bmod 5 = 4\\
&2 \cdot 3 \bmod 5 = 6 \bmod 5 = 1\\
&2 \cdot 4 \bmod 5 = 8 \bmod 5 = 3\\
&2 \cdot 5 \bmod 5 = 10 \bmod 5 = 0\\
&2 \cdot 6 \bmod 5 = 12 \bmod 5 = 2\\
&2 \cdot 7 \bmod 5 = 14 \bmod 5 = 4\\
&\vdots
\end{aligned}$$

We make two observations: the first is that all the elements of $\mathbb{Z}_5$ are reached through powers of 2, thus we have proven that it is generated by 2. The second is that, after $2 \cdot 5$, it is clear that the numbers start to repeat in a fixed order. That is, the powers of 2 cycle through $\mathbb{Z}_5$ in the order $0, 2, 4, 1, 3$. Note that generators are not unique. For example, $\mathbb{Z}_5$ could be generated by 1 as well, although not by 0.

Moreover, although we will not get into the technical details, we informally mention that any cyclic group of finite order n behaves like the additive group $\mathbb{Z}_n$, and any cyclic group of infinite order behaves like $\mathbb{Z}$.

Proposition 6.1. For any $n \in \mathbb{N}$, we have that $(\mathbb{Z}_n, +)$, where $+$ is addition modulo n, is a cyclic group.

Exercise 6.2. *Decide whether the group $\mathbb{Z}_2 \times \mathbb{Z}_3$, with component-wise modular addition, is a cyclic group.*

Groups might contain smaller groups inside, that are consistent with the same operation.

Definition 6.3. *Let $\mathbb{G}$ be a group. A* subgroup $\mathbb{H}$ *of $\mathbb{G}$ is a subset of $\mathbb{G}$ that contains the identity element and such that $\mathbb{H}$ forms a group with the operation of $\mathbb{G}$ restricted to $\mathbb{H}$. That is, for any $x, y \in \mathbb{H}$, we have that $x^{-1} \in \mathbb{H}$ and $xy \in \mathbb{H}$.*

For example, the set of even integers is a subgroup of $(\mathbb{Z}, +)$, since the addition of even numbers is even. It is easy to see that subgroups are groups too.

Exercise 6.3. *Decide which of these subsets are subgroups of $(\mathbb{Z}_4, +)$:*

$$\{0\}, \qquad \{0, 2\}, \qquad \{1, 3\}, \qquad \{0, 1, 3\}.$$

It is easy to see that, for any $x \in \mathbb{G}$, the group $\langle x \rangle$ is a subgroup of $\mathbb{G}$. Note that this might not be the whole $\mathbb{G}$. This allows us to define the order of an element as follows.

Definition 6.4. *Let $\mathbb{G}$ be a group, and $x \in \mathbb{G}$. We define the* order *of x as the order of $\langle x \rangle$, and denote it by $ord(x)$.*

The following Sage code defines the additive group $(\mathbb{Z}_9, +)$, computes a generator, and then computes the order of each element, also explicitly providing the cycle that corresponds to that element.

```
G = AdditiveAbelianGroup([9])
g = G_add.gens()[0]           # The [0] is necessary because, technically,
                              # .gens() returns a list.
print(str(G)+", generator: "+str(g))
for x in G:
    print("x = "+str(x)+", ord(x) = "+str(x.order()))
    for i in range(x.order()+1):
        print(i*x)
```

If $\mathbb{H}$ is a subgroup of $\mathbb{G}$, it is clear that the order of $\mathbb{H}$ will be smaller than the order of $\mathbb{G}$, since the former is contained in the latter. But even more, it will necessarily be a divisor, which is something you may have observed after running the above code.

Proposition 6.2 (Lagrange's theorem)**.** Let $\mathbb{G}$ be a finite group.

For any subgroup $\mathbb{H}$ of $\mathbb{G}$, $ord(\mathbb{H}) \mid ord(\mathbb{G})$.

For any $x \in \mathbb{G}$, $ord(x) \mid ord(\mathbb{G})$.

The order of a group plays an important role in the group operation.

Proposition 6.3 (Euler's theorem)**.** Let $\mathbb{G}$ be a group of finite order. Then, for any $x \in \mathbb{G}$, we have that

$$x^{ord(\mathbb{G})} = 1.$$

Exercise 6.4. *Verify that Euler's theorem holds for the group $\mathbb{Z}_7^*$, with the operation multiplication modulo 7.*

The exercise can also be solved with Sage, using the following code.

```
G = Integers(7).unit_group()     # Multiplicative group Z_7^*.
for x in G:
    print(x^(G.order()))
```

These propositions give us an easy way to check whether an element $x \in \mathbb{G}$ is a generator. Recall that the order of x tells us how many elements there are in

$$\langle x \rangle = \{x^n \mid n \in \mathbb{Z}_{\geq 0}\},$$

that is, the number of steps in the cycle of powers of x before going back to 1 and repeating elements. If it were the case that $ord(x) = ord(\mathbb{G})$, this would mean that a the cycle is as big as $\mathbb{G}$, and therefore it must be that $\langle x \rangle = \mathbb{G}$. On the other hand, if $ord(x) < ord(\mathbb{G})$, this would mean that not all elements of $\mathbb{G}$ can be obtained as powers of x, and thus x would not generate $\mathbb{G}$.

Hence, we can check whether x generates $\mathbb{G}$ by computing $ord(x)$ and comparing it with $ord(\mathbb{G})$. To do so, a naive approach would be to iteratively compute

$$x, x^2, x^3, x^4, x^5, \ldots$$

until some n is found such that

$$x^n = 1,$$

and we would have that $n = ord(x)$. However, note that this approach takes time linear in $ord(\mathbb{G})$. When $ord(\mathbb{G})$ is easy to factor, a more sensible approach is to use Lagrange's theorem, which tells us that

$$ord(x) \mid ord(\mathbb{G}).$$

This allows us to drastically reduce the candidates to the powers

$$x^{\frac{ord(\mathbb{G})}{d}},$$

for all $d \mid ord(\mathbb{G})$. The smallest exponent that produces a 1 will be the order of x. In particular, if $ord(G)$ is prime, then there are only two candidates: x and $x^{ord(\mathbb{G})}$. Hence in this case, if $x \neq 1$, necessarily x is a generator. That is, we have proven the following result.

Proposition 6.4. Let $\mathbb{G}$ be a cyclic group of prime order. If $g \in \mathbb{G}$ is not the identity element, then g generates $\mathbb{G}$.

We conclude the section on groups by looking at some specific properties of the groups $\mathbb{Z}_n$ and $\mathbb{Z}_n^*$.

Proposition 6.5. Let p be a prime number. The multiplicative group $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$, and it has $\varphi(p-1)$ generators. These generators are called *primitive roots* modulo p.

Moreover, a direct consequence of Euler's theorem and the proposition above is known as *Fermat's little theorem*.[2]

[2]Not to be confused with *Fermat's last theorem*, which states that there are no positive integer solutions for the equation $x^n + y^n = z^n$ for any integer $n > 2$. This theorem has become famous due to its history: it was originally claimed by Pierre de Fermat in the 17th century. He wrote it in the margin of a book, claiming to know a proof but lacking the space to write it down. Such proof was never found, and the first known proof of the theorem appeared more than three centuries later, in the 1990s, when Andrew Wiles finally solved the problem, after the contributions of a long lineage of mathematicians.

Proposition 6.6 (Fermat's little theorem)**.** Let p be a prime number. Then, for any $x \in \mathbb{Z}$, we have that

$$x^{p-1} \equiv 1 \pmod{p}.$$

6.2 Finite fields

A *field* is a more complex algebraic structure, since it is equipped with two operations, both of which work similarly to a group operation.[3]

Definition 6.5. *A* field *is a triple* $(\mathbb{F}, \circ, *)$*, where* $\mathbb{F}$ *is a set and* $\circ$ *and* $*$ *are operations on* $\mathbb{F}$*, that is, functions*

$$\begin{aligned} \circ : \ \mathbb{F} \times \mathbb{F} &\to \mathbb{F} \\ (x, y) &\mapsto x \circ y, \end{aligned} \qquad \begin{aligned} * : \ \mathbb{F} \times \mathbb{F} &\to \mathbb{F} \\ (x, y) &\mapsto x * y, \end{aligned}$$

which additionally satisfy the following properties:

1. $(\mathbb{F}, \circ)$ *is a commutative group, with identity element denoted by* 0*.*
2. $(\mathbb{F} \setminus \{0\}, *)$ *is a commutative group, where* $\mathbb{F} \setminus \{0\}$ *is the set* $\mathbb{F}$ *except for the identity element of* $\circ$*.*
3. Distributive law: $x * (y \circ z) = (x * y) \circ (x * z)$ *for all* $x, y, z \in \mathbb{F}$*.*

Since we have two operations at the same time, we will adopt the additive and multiplicative notation from groups to represent each of them, respectively. That is, we will think of the first operation of a field as a form of *addition* and the second as a form of *multiplication*. On input x, y, we write the result of the first operation by $x + y$, and the result of the second by xy. The identity elements of each operation are denoted by 0 and 1, respectively. The inverse of x with respect to the first operation is denoted by $-x$. The inverse of x with respect to the second operation is denoted by x^{-1}. The following table summarizes the notation:

Operation	Operation on input x, y	Identity element	Inverse of x
$+$	$x + y$	0	$-x$
$\cdot$	xy	1	x^{-1}

[3] Appendix A contains a more detailed introduction to this section. It first defines another algebraic structure called a *ring*, which is somewhat between a group and a field, and then defines fields as a particular type of ring. This appendix is not part of the content for the exam, and the main body of these notes is designed to be self-contained, but nevertheless we advise you to read Appendix A before reading about fields, since it provides a more natural introduction to the topic.

We consider some examples:

- $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, with usual addition and multiplication, are fields. The properties are easy to check. Identity elements are 0 and 1. The additive inverse of x is $-x$, and the multiplicative inverse of x is $1/x$.
- Consider $\mathbb{Z}_9$, with addition and multiplication modulo 9. It satisfies most of the properties of a field, but we will see that some elements have no inverse with respect to the second operation. The following table gives the multiplicative inverses of each element:

x	0	1	2	3	4	5	6	7	8
x^{-1}	–	1	5	–	7	2	–	4	8

  Note that some elements are not invertible, in this case 0, 3 and 6. Therefore, $\mathbb{Z}_9$ is not a field.

In Sage, the following code can be used to check whether an element of $\mathbb{Z}_n$ has a multiplicative inverse.

```
R = Integers(n)      # Z_n with addition and
                     # multiplication modulo n.
for x in R:
    print(x,x.is_unit())
```

In this course we will be interested in *finite fields*,[4] so what are some examples of those? Could it be, for example, that $\mathbb{Z}_n$ is a field for some $n \in \mathbb{N}$? We already know that this will not be true for all $n \in \mathbb{N}$, since we saw that some elements of $\mathbb{Z}_9$ do not have an inverse.

Proposition 6.7. The $\mathbb{Z}_n$, with addition and multiplication modulo n, is a field if and only if n is a prime number.

The only finite fields that exist have a number of elements that is either a prime number or a power of a prime number.

Proposition 6.8. Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}$ has p^k elements, where p is a prime number and $k \in \mathbb{N}$. We denote such a finite field by $\mathbb{F}_{p^k}$. If $k = 1$, the field is called a *prime field*, otherwise it is known as an *extension field*. We call p the *characteristic* of the field.

[4] Sometimes also called Galois fields, after the mathematician Évariste Galois, who notably proved that there is no algebraic formula for solving polynomial equations of degree higher than 4, and then died after a duel at the age of 20.

Moreover, given a prime p and $k \in \mathbb{N}$, there is essentially only one field with p^k elements, although this same field can have different representations.

One might think that these extension fields $\mathbb{F}_{p^k}$ correspond to $\mathbb{Z}_{p^k}$, but actually this is not true. Again, we recall the example in which we showed that $\mathbb{Z}_9 = \mathbb{Z}_{3^2}$ is not a field, because some elements are not invertible. So, if $\mathbb{F}_{p^k}$ is not $\mathbb{Z}_{p^k}$, what is it?

It turns out that we need some more involved tools to describe these. An element of the field $\mathbb{F}_{p^k}$ is not represented by an integer. Instead, we use a polynomial

$$r_{k-1}x^{k-1} + \cdots + r_1 x + r_0,$$

for some coefficients $r_{k-1}, \ldots, a_0 \in \mathbb{F}_p$. Note that the degree of the polynomial is $k-1$ for representing an element of $\mathbb{F}_{p^k}$. Since there are k coefficients, and each of these has p possible values, we see that there are in total p^k possible polynomials, and thus so far it makes sense to try to associate these with the p^k elements of $\mathbb{F}_{p^k}$.

But we still need to specify how the operations work. For addition, we use usual polynomial addition, that is,

$$\begin{aligned} R(X) + S(X) &= (r_{k-1}X^{k-1} + \cdots + r_1 X + r_0) + (s_{k-1}X^{k-1} + \cdots + s_1 X + s_0) = \\ &= (r_{k-1} + s_{k-1})X^{k-1} + \cdots + (r_1 + s_1)X + (r_0 + s_0), \end{aligned}$$

which is also a polynomial of degree at most $k-1$, and it is easy to see that it verifies the conditions of a group operation. Note that the coefficients are in $\mathbb{F}_p$, so the additions of the coefficients are reduced modulo p if necessary.

For multiplication, we consider multiplying the two polynomials. However, note that, in general, multiplying two polynomials $R(X)$ and $S(X)$ of degree $k-1$ produces a polynomial $R(X)S(X)$ of degree $2k-2$, which is not in $\mathbb{F}_{p^k}$ anymore. Our trick then is analogous to what we did in $\mathbb{F}_p = \mathbb{Z}_p$. In that case, we reduced the result modulo a prime number p. Now, we will reduce the result modulo a certain polynomial $T(X)$ of degree k. This means that we compute the polynomial division of $R(X)S(X)$ by $T(X)$, and keep the remainder, so that the result has degree at most $k-1$.[5] Since this is analogous to the case of integers, we extend the notation

$$A(X) \bmod T(X)$$

to denote the remainder of the polynomial division $A(X)$ by $T(X)$, and the notation

$$A(X) \equiv B(X) \pmod{T(X)}$$

to denote that

$$(A(X) - B(X)) \bmod T(X) = 0,$$

[5] See Appendix C.4 for a refresher on how to perform polynomial division.

that is, $A(X) - B(X)$ is a multiple of $T(X)$.

But which polynomial $T(X)$ should we use? Not every polynomial will yield a multiplication law of a field. We require an *irreducible polynomial*, that is, a polynomial that cannot be written as a product of two non-trivial polynomials with coefficients in $\mathbb{F}_p$.

At first, this might seem like an obscure condition, but if you think about it, it is actually analogous to what happened for prime fields. In that case, we started from $\mathbb{Z}_n$, and concluded that it is only a field when n is a prime, which is precisely a number that cannot be factored in a non-trivial way. In extension fields, we are representing elements by polynomials instead of integers, and so we look for the analogue of a prime number in this sense of lack of factorization. This leads us to irreducible polynomials, although a formal proof of this statement is beyond the scope of this course.

Proposition 6.9. Let p be a prime number and $k \in \mathbb{N}$. Let $T(X)$ be an irreducible polynomial of degree k with coefficients in $\mathbb{F}_p$. The set of polynomials of degree at most $k-1$ and coefficients over $\mathbb{F}_p$, together with the operations polynomial addition and multiplication modulo $T(X)$, is a field of p^k elements.

The choice of irreducible polynomial $T(X)$ determines the multiplication law, but any of the outcomes can be seen as different representations of the same finite field of size p^k.

Finally, inversion of elements in $\mathbb{F}_{p^k}$ can be handled with the extended Euclidean algorithm por polynomials, similarly to the way it was used to invert integers modulo n. We describe this algorithm below.

Definition 6.6. *Given a polynomial*

$$a_k X^k + a_{k-1} X^{k-1} + \cdots + a_1 X + a_0,$$

we define its leading coefficient *as the coefficient of the highest-degree monomial, in this case a_k. A polynomial with leading coefficient 1 is called* monic.

Definition 6.7. *Given two polynomials $A(X)$ and $B(X)$, we define their* greatest common divisor *as the highest-degree monic polynomial that divides both.*

Proposition 6.10. Let p be a prime number and let $k \in \mathbb{N}$. Let $\mathbb{F}_{p^k}$ be the finite field of p^k elements, with irreducible polynomial $T(X)$. Let $A(X), B(X)$ be two elements of $\mathbb{F}_{p^k}$. Then, there exist $U(X), V(X)$ in $\mathbb{F}_{p^k}$ such that

$$A(X)U(X) + B(X)V(X) = \gcd(A(X), B(X)).$$

The Euclidean algorithm for polynomials is very similar to the analogous algorithm for integers, with an additional step to ensure that the output is a monic polynomial.

1. Compute the polynomial division of $A(X)$ by $B(X)$, obtaining $Q(X), R(X)$ such that the $0 \leq \deg R < \deg B$ and
$$A(X) = B(X)Q(X) + R(X).$$
2. If $R(X) = 0$, go to step 3. Otherwise, return to the previous step, replacing $A(X)$ by $B(X)$ and $B(X)$ by $R(X)$.
3. Multiply $B(X)$ by the inverse of its leading coefficient, and output the result.

This will produce $\gcd(A(X), B(X))$, from which we can go back through the procedure to find the expression in the proposition above. We show an example in $\mathbb{F}_{5^4}$, with irreducible polynomial $T(X) = X^4 + 4X^2 + 4X + 2$.

$$A(X) = X^3 + 3X^2 + 4, \qquad B(X) = X^2 + 2X + 2.$$

Note that coefficients are in $\mathbb{F}_5$, and thus all the operations performed on coefficients must be carried out modulo 5. We start by dividing $A(X)$ by $B(X)$, obtaining
$$X^3 + 3X^2 + 4 = (X^2 + 2X + 2)(X + 1) + (X + 2)$$
Since the remainder is not 0, we compute the next polynomial division, obtaining
$$X^2 + 2X + 2 = (X + 2)X + 2.$$
Finally,
$$(X + 2) = 2(3X + 1) + 0.$$
Since the last remainder is 0, we conclude that the greatest common divisor of $A(X)$ and $B(X)$ is 2 multiplied by the inverse of its leading coefficient, so in this case
$$\gcd(A(X), B(X)) = 2 \cdot 2^{-1} = 1.$$
Again, by undoing these steps, we can find the expression in Proposition 6.10:
$$2 = (X^2 + 2X + 2) - (X + 2)X.$$
We also have that
$$X + 2 = (X^3 + 3X^2 + 4) - (X^2 + 2X + 2)(X + 1),$$
and thus, combining the two expressions,
$$\begin{aligned} 2 &= (X^2 + 2X + 2) - \big((X^3 + 3X^2 + 4) - (X^2 + 2X + 2)(X - 1)\big)\, X = \\ &= (X^2 + 2X + 2) - (X^3 + 3X^2 + 4)X + (X^2 + 2X + 2)(X^2 + X) = \\ &= (-X)(X^3 + 3X^2 + 4) + (X^2 + X + 1)(X^2 + 2X + 2). \end{aligned}$$

Multiplying both sides by $2^{-1} \bmod 5 = 3$, we have that

$$\begin{aligned} 1 &\equiv (-3X)(X^3 + 3X^2 + 4) + (3X^2 + 3X + 3)(X^2 + 2X + 2) \equiv \\ &\equiv (2X)(X^2 + 3X^2 + 4) + (3X^2 + 3X + 3)(X^2 + 2X + 2). \end{aligned}$$

Therefore,

$$U(X) = 2X, \qquad V(X) = 3X^2 + 3X + 3.$$

As in the case of integers, we can compute the inverse of $A(X)$ in $\mathbb{F}_{p^k}$ by running the Extended euclidean algorithm on $A(X)$ and the irreducible polynomial $T(X)$, obtaining some polynomials $U(X), V(X)$ such that

$$1 = A(X)U(X) + T(X)V(X),$$

thus

$$1 \equiv A(X)U(X) \pmod{T(X)},$$

and we find that $U(X)$ is the inverse of $A(X)$ in $\mathbb{F}_{p^k}$.

We show to define and manipulate finite fields in Sage.

```
# Finite field of size 3^5. The optional argument modulus=p
# allows to specify the irreducible polynomial p to be used.
F = GF(3^5, "X")
F

# Get the polynomial p(X)=X into the field.
X = F("X")

# Show the irreducible polynomial being used.
F.modulus()

# Define two elements of F and operate with them.
a = F(X^4+X^2+2*X)
b = F(2*X^2+2*X^3+1)
# Addition
print("a + b = "+str(a+b))
# Multiplication
print("a * b = "+str(a*b))
# Inversion
print("a^{-1} = "+str(a^(-1)))
```

Chapter 7

Public-key encryption

Equipped with the mathematical tools developed in the previous two chapters, we are now in a position to introduce the concept of public-key cryptography, and present some of the best-known constructions in this setting. More precisely, we will learn about:

- The paradigm of public-key cryptography.
- The RSA encryption scheme and its security.
- The ElGamal encryption scheme and its security.

7.1 Public-key cryptography

In Section 1, we introduced a symmetric encryption scheme, in which two parties use a shared secret key to communicate privately. We still have not solved the problem of establishing this common key in a secure way. We will now introduce a new type of encryption scheme, which stems from the following idea: what if we don't need a shared secret key to have secure communications? This idea was introduced by Diffie and Hellman in the renowned paper *New directions in cryptography*,[1] which is considered to be the birth of modern cryptography.

They introduced the notion of *asymmetric* or *public-key* encryption, which on a high level works as follows. Imagine that Alice wishes to send a message to Bob. Bob produces two keys pk and sk, crafted in such a way that whatever is encrypted with pk can be decrypted only with sk. That is, for any message m,

$$\mathsf{Dec}_{\mathsf{sk}}\left(\mathsf{Enc}_{\mathsf{pk}}(\mathsf{m})\right) = \mathsf{m}.$$

[1] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6), 644-654.

Then Bob publishes pk, so that anyone can know it, and keeps sk secret. For this reason, pk is known as Bob's *public key* and sk is Bob's *secret key*.

Definition 7.1. *An* asymmetric (or public-key) encryption scheme *is composed of three efficient algorithms:*

$$(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}).$$

- *The* KeyGen *algorithm chooses two keys* pk, sk *of length* λ*, according to some probability distribution, and such that*

$$\mathsf{Dec}_{\mathsf{sk}}\left(\mathsf{Enc}_{\mathsf{pk}}(\mathsf{m})\right) = \mathsf{m}.$$

- *The* Enc *algorithm uses the public key* pk *to encrypt a message* m*, and outputs the encrypted message*

$$\mathsf{c} = \mathsf{Enc}_{\mathsf{pk}}(\mathsf{m}).$$

- *The* Dec *algorithm uses the secret key* sk *to decrypt an encrypted message* c*, recovering* m *as*

$$\mathsf{Dec}_{\mathsf{sk}}(\mathsf{c}) = \mathsf{m}.$$

In this context, m *is called the* plaintext*, and* c *is said to be its corresponding* ciphertext*. The keys* pk *and* sk *are the* public key *and* secret key*, respectively.*

Note that, for such a construction to be secure, we need that the secret key cannot be efficiently computed from the public key. Otherwise, since the public key is known to everybody, in particular attackers, this could be exploited to recover the secret key and decrypt any message.

Another difference with symmetric encryption is that the structure of the keys is different. In symmetric encryption, we had a key associated to two parties, Alice and Bob, which was used to send messages both ways. But, in the explanation above, we just described how Alice sends messages to Bob, but not the other way around. Note that if Bob tried to use sk to encrypt, with the hope that Alice decrypts with pk, then anybody would be able to decrypt, since pk is public. Therefore, Alice needs another pair of keys, one public that is used for everybody else to encrypt messages to Alice, and one secret, that is used by Alice to decrypt messages addressed to her.

This might seem like a downgrade, since before we needed only one key and now we have four in total. We emphasize, however, that none of the secret keys need to be shared, and the public ones can be shared through an insecure channel. Moreover, we actually have less keys in the asymmetric case when many parties are involved, as is highlighted by the following exercise.

Exercise 7.1. *Suppose that we have* n *parties, and each of them wishes to communicate with all the others. Compute how many keys are needed if they use:*

1. *A symmetric encryption scheme.*
2. *A public-key encryption scheme.*

7.2 The RSA encryption scheme

Although Diffie and Hellman introduced the idea of public-key encryption in 1976, it was not until 1978 that Rivest, Shamir and Adleman published the first public-key encryption scheme, which became known as the RSA encryption scheme.[2] The scheme works as follows.

- KeyGen: on input a security parameter λ, choose two uniformly random prime numbers p, q of bitlength $\lambda/2$, and let $N = pq$. We will work in $\mathbb{Z}_N$, and call N an *RSA modulus*. Choose $e \in \mathbb{Z}_N$, and compute

$$d \equiv e^{-1} \pmod{\varphi(N)}.$$

  Output the public key

$$\mathsf{pk} = (N, e),$$

  and the secret key

$$\mathsf{sk} = d.$$

  Note that it is crucial that p, q are uniformly random, whereas e can be a fixed parameter.[3]

- Enc: given a message $\mathsf{m} \in \mathbb{Z}_N$, and the receiver's public key (N, e), output a ciphertext

$$\mathsf{m}^e \bmod N.$$

- Dec: given a ciphertext c and the secret key d, output

$$\mathsf{c}^d \bmod N.$$

There are a few things to consider here. The first is, why does this even work? That is, how can we be sure that the original message is recovered after encryption and decryption. We observe that, given a message m, we have that

$$\mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(\mathsf{m})) = \mathsf{Dec}_{\mathsf{sk}}(\mathsf{m}^e \bmod N) = (\mathsf{m}^e)^d \bmod N = \mathsf{m}^{ed} \bmod N.$$

Now, we use that

$$d \equiv e^{-1} \pmod{\varphi(N)},$$

[2] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.

[3] Initially, it was suggested to use $e = 3$ for efficiency, although this opened the gates to some attacks. Nowadays, the most common option is $e = 2^{16} + 1$.

which means that there is an integer k such that

$$de = k\varphi(N) + 1.$$

Thus, by plugging this into the expression above, we have

$$\mathsf{m}^{ed} \bmod N = \mathsf{m}^{k\varphi(N)+1} \bmod N = \left(\left(\mathsf{m}^{\varphi(N)}\right)^k \cdot \mathsf{m}\right) \bmod N.$$

Finally, we use Euler's theorem (Proposition 6.3) and Proposition 6.5, which tell us that

$$\mathsf{m}^{\varphi(N)} \bmod N = 1,$$

and therefore

$$\mathsf{m}^{ed} \bmod N = \mathsf{m}.$$

This proves that decryption indeed reverses encryption.

A second consideration is: are the three algorithms involved efficient? It is easy to see that Enc and Dec are efficient, since they amount to one modular exponentiation each, which we have seen that is an efficient computation (Section 5.4). Let us analyze the KeyGen algorithm by breaking it into these steps:

1. Sample prime numbers of size λ.
2. Compute $N = pq$.
3. Compute $\varphi(N)$.
4. Compute the inverse of e modulo $\varphi(N)$.

Step (1) can be further broken into two parts: sample a random number of length λ, and recognize whether it is a prime or not. We know we can sample random numbers efficiently and, as discussed in Section 5.1 and Appendix B, there are efficient algorithms to determine the primality of a number.[4]

So the strategy is to sample random numbers until we find a prime. But how many tries do we need? The prime number theorem (Proposition 5.3) tells us that, for large numbers, the amount $\pi(n)$ of primes up to n is roughly $n/\log n$ which means that the probability of a random number being a prime is approximately $1/\log n$. This means that, on average, we will need $\log n = O(\lambda)$ tries before finding a prime. Thus, the total cost of step (1) is $O(\lambda^3)$.

Step (2) is simple arithmetic, which is efficient. Computing $\phi(N)$ in step (3) is easy when knowing the factorization of N since, if $N = pq$, then

$$\varphi(N) = (p-1)(q-1),$$

[4] In practice, most of the time we use the Miller–Rabin algorithm, which runs in time $O(\lambda^2)$, although it can produce false positives with a very small probability. A completely fail-safe alternative is the AKS algorithm, which is still efficient but much slower. More detail can be found in Appendix B.

as a consequence of Proposition 5.8. Finally, step (4) can be performed efficiently using the Euclidean algorithm.

The following Sage code is a very simple implementation of the three algorithms composing the RSA encryption scheme.

```
# Set a security parameter
sec_param = 1024

### KEY GENERATION
# Generate two prime numbers of length sec_param/2
p = random_prime(2^(sec_param/2-1),2^(sec_param/2)-1)
q = random_prime(2^(sec_param/2-1),2^(sec_param/2)-1)
# Set the RSA modulus:
N = p*q
# Compute Euler's phi function on N:
phi = (p-1)*(q-1)
# Define Z_N, so that all operations are
# automatically reduced modulo N.
Z = Integers(N)
# Choose a public key:
e = 2^16 + 1
# Compute the corresponding secret key:
d = inverse_mod(e,phi)       # Euclidean algorithm is used under the hood.

### ENCRYPTION - using pk = (N,e)
# Choose a message to encrypt.
m = 176670438034866691434474384362513673776640000854515104842048092159098845565020566033048860134
# Check that the message fits in Z_N.
if (m >= N):
    print("Message too large.")
else:
    # Encrypt the message
    c = Z(m)^e      # Z(m) is written instead of m so that Sage recognizes m
                    # as an element of Z_N, and performs operations modulo N.
    print("c = "+str(c))


### DECRYPTION - using sk = d
m = Z(c)^d
print("m = "+str(m))
```

Exercise 7.2. *In the code above, can we replace the line about computing $\varphi(N)$ by* `phi = euler_phi(N)`*?*

7.3 Security of RSA

So we know that the scheme works and is efficient. It remains to discuss security. As mentioned above, the secret key should be hard to deduce from the public key, otherwise anyone would have access to it, and thus anyone would be able to decrypt.

By looking again at the generation of the secret key in KeyGen, we observe that it can be computed from e and $\varphi(N)$. The parameters e and N are public, so what prevents attackers from computing the secret key? The crucial point is that, in KeyGen, we were able to compute $\varphi(N)$ from the *factorization* (p, q) of N, by computing

$$\varphi(N) = (p-1)(q-1).$$

However, if we do not know the factors of N, we cannot carry out this computation. Moreover, this works both ways: it can be shown that knowledge of $\varphi(N)$ allows to factor N efficiently. Thus, the security of RSA relies on the hardness of factorization.

Definition 7.2. *Let p, q be large prime numbers, and let $N = pq$. The* factorization problem *consists of recovering p, q, given N.*

As mentioned in Section 5.1, there is no known algorithm for factoring a product of two large primes efficiently.

Hardness of factorization is a necessary condition for security but, unfortunately, not a sufficient one. That is, an adversary could still in principle decrypt a ciphertext without the need of the secret key, with some other technique. This motivates the introduction of the following problem.

Definition 7.3. *Let p, q be large primes, and let $N = pq$. Let $e \in \mathbb{Z}_N$. The* RSA problem *consists of recovering $\mathsf{m} \in \mathbb{Z}_N$, given N, e and $\mathsf{m}^e \bmod N$.*

Clearly if factorization is easy then the RSA problem is also easy, but the implication in the other direction is not known to be true or false so far. However, as is the case with the factorization problem, there have been extensive attacks against the RSA problem, and no better attack than factorization of N has been found. This provides a reasonable guarantee that the problem is indeed hard, even if we lack a formal proof.

For security against current computational power, most organizations suggest a security parameter of at least $\lambda = 2048$ (see https://www.keylength.com/). That is, an RSA modulus N of bitlength 2048 is believed to be secure against current factorization attempts. To date, the highest RSA modulus to be factored has bitlength 829, and took about 2700 core-years.[5]

So is this enough to call the RSA scheme secure? Unfortunately, no, since it is vulnerable to other attacks that do not depend on recovering the secret key.

[5] https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html

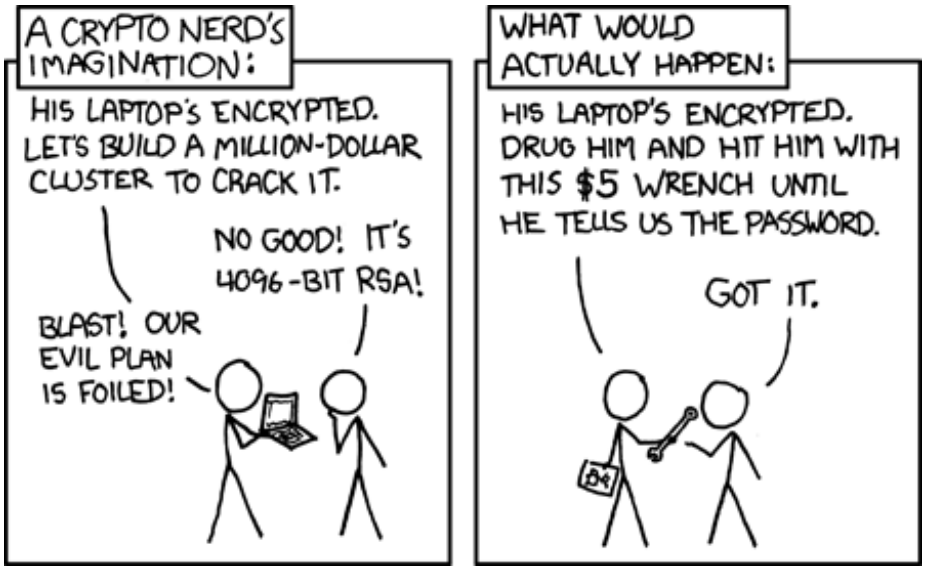


Figure 7.1: Webcomic by xkcd (https://xkcd.com/538/).

We consider the following scenario: suppose that Alice is sending Bob a date of the year, in the format $DDMM$, where DD is the day and MM is the month. An attacker knows this, and also has access to Bob's public key (N, e), since anyone can obtain public keys. The attacker eavesdrops the ciphertext `c` that Alice sends Bob, and then computes

$$(DDMM)^e \bmod N$$

for each $DD \in \{1, \ldots, 31\}$ and $MM \in \{1, \ldots, 12\}$. The attacker compares the list of results with `c` until they find a match, which tells them the date that was encrypted in `c`. This is known as a *chosen-plaintext attack (CPA)*, since the adversary can obtain the encryptions of messages of their own choice. More precisely, we introduce the following definition.

Below is some code for running this attack. As an attacker, we have access to the security parameter λ, the RSA modulus `N`, and the encryption exponent `e`. We intercept some ciphertext `c`, and run the attack by comparing `c` with the encryption of each possible message.

```
### Auxiliary function
# Write day/month in the format DDMM
def format(day,month):
    day = str(day)
    month = str(month)
    if len(day)<2:
```

```
        day = "0" + day
    if len(month)<2:
        month = "0" + month
    return int(day + month)


### CPA attack
# Known data
N = 508492348634291983774915882645435640334656925998167110618633324491507315577007606995
Z = Integers(N)
e = 2^16 + 1
# Intercepted ciphertext
c = 10560507325761782128927466270697576111440545183685933602207062946482651138016518513

# Running the attack
for month in range(1,13):
    for day in range(1,32):
        m = format(day,month)
        c_candidate = Z(m)^e
        if c_candidate == c:
            print("Recovered plaintext: "+str(m))
```

The version of RSA described above is known as *textbook RSA*, because it is a version simplified for didactic purposes, but is not secure against chosen-plaintext attacks, and thus not secure for real-world use.

How could such an attack happened? We boil it down to three facts:

1. The receiver's public key is known by the attacker, so the attacker can compute ciphertexts of messages of their choice.
2. The set of possible messages is small, so it is efficient for the attacker to compute ciphertexts of every possible message.
3. The encryption algorithm was deterministic, so the attacker can compare their list of ciphertexts with the intercepted ciphertext and find a match. Recall Principle 3 from the beginning of the course: there is no security without randomness.

Fact (1) happens by design of public-key schemes. There is not much we can do about fact (2) either, since a good encryption scheme should allow users to communicate any data. Therefore, to fix RSA we need to do something about fact (3).

The idea is to modify the message before running it through the RSA encryption algorithm, and add some randomness to it. There are many different proposals

to achieve this, collectively known as *padded RSA*. We describe one successful variant known as *RSA-OAEP*.[6]

Unfortunately, it is not as simple as appending some random bits at the end of the message, and we need a more involved process. Let

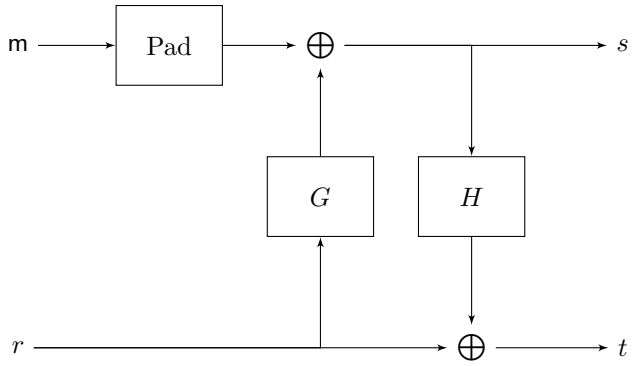
$$G : \{0,1\}^{k_0} \to \{0,1\}^{\ell+k_1}, \qquad H : \{0,1\}^{\ell+k_1} \to \{0,1\}^{k_0}$$

be two hash functions, where k_0, k_1 are such that $\lambda = O(k_0)$ and $\lambda = O(k_2)$, and $\ell + k_0 + k_1$ is smaller than the bitlength of N. We describe how to modify a message m of bitlength ℓ. We introduce randomness by uniformly sampling a bitstring $r \in \{0,1\}^{k_0}$, and then compute:

$$s = \mathsf{m}|\mathbf{0}^{k_1} \oplus G(r), \qquad t = r \oplus H(s),$$

where $\mathsf{m}|\mathbf{0}^{k_1}$ is the bitstring m, concatenated with the string of zeros of length k_1. Then, we set the new message as $\hat{\mathsf{m}} = (s,t)$, which is then run through textbook RSA. Observe that $s \in \{0,1\}^{\ell+k_1}$ and $t \in \{0,1\}^{k_0}$, so the message $\hat{\mathsf{m}}$ has the appropriate length.

We summarize the construction in the following diagram.



Exercise 7.3. *Describe the decryption procedure that corresponds to RSA-OAEP.*

With these modifications, we can finally claim that the RSA cryptosystem is secure.

Proposition 7.1. If the RSA problem is hard and G and H behave as ideal[7] hash functions, then the RSA-OAEP encryption scheme is secure.

[6] OAEP stands for *optimal asymmetric encryption padding*.

[7] Essentially, this means that the hash functions output uniformly random elements of their respective codomains. This is not true for actual hash functions, but it does not make a difference in practice.

Note that the textbook version of RSA is also *malleable*. This means that, given a ciphertext of some message, it is easy to produce a ciphertext of a related message. For example, given a ciphertext c for the message m, i.e.

$$\mathsf{c} = \mathsf{m}^e \bmod N,$$

an adversary can compute

$$\mathsf{c}' = 2^e \mathsf{c} \bmod N = (2\mathsf{m})^e \bmod N,$$

which is a valid ciphertext for the message $2\mathsf{m} \bmod N$. The OAEP transformation also makes the scheme non-malleable.

7.4 Efficiency optimizations

As discussed above, the algorithms involved in RSA are all efficient, although not particularly fast. In this section, we look at some efficiency tricks to speed up the computations.

A simple one is to choose the encryption exponent e so that its binary representation has many zeros. This has an impact on the computation of the exponentiation when the square-and-multiply algorithm (Section 5.4) is used. Recall that, for each bit, the algorithm consists of one squaring and, if the bit is 1, one multiplication, both operations modulo n. By choosing an exponent like $e = 2^n + 1$, with binary representation

$$[e]_2 = 1\underbrace{0\ldots0}_{n-1}1,$$

we ensure that we skip most of the multiplications. In practice, often the exponent $2^{16} + 1$ is chosen.

Another possible optimization is to make use of the Chinese remainder theorem (Proposition 5.9), and perform the operations in $\mathbb{Z}_p$ and $\mathbb{Z}_q$, and then reconstruct the plaintext in $\mathbb{Z}_N$, instead of working in $\mathbb{Z}_N$ directly. Since p, q are half the size of N, exponentiations are cheaper here, and overall the procedure is roughly four times faster. More precisely, let $\mathsf{c} \in \mathbb{Z}_N$ be a ciphertext, and let $d \in \mathbb{Z}_N$ be the secret key. We compute

$$\begin{aligned} \mathsf{c}_p &= \mathsf{c} \bmod p & \mathsf{c}_q &= \mathsf{c} \bmod q, \\ d_p &= d \bmod \varphi(p), & d_q &= d \bmod \varphi(q), \end{aligned}$$

and use these to decrypt in $\mathbb{Z}_p$ and $\mathbb{Z}_q$:

$$\mathsf{m}_p = \mathsf{c}_p^{d_p} \bmod p, \qquad \mathsf{m}_q = \mathsf{c}_q^{d_q} \bmod q.$$

Now, we have m_p and m_q, and the Chinese remainder theorem tells us that there is a unique $\mathsf{m} \in \mathbb{Z}_N$ such that

$$\mathsf{m} \equiv \mathsf{m}_p \pmod p, \quad \mathsf{m} \equiv \mathsf{m}_q \pmod q,$$

and the second part of the theorem gives us a formula to explicitly recover such m.

Chapter 8

Discrete logarithm cryptosystems

In the previous lesson, we saw that the security of the RSA encryption scheme relies on the hardness of factoring products of two large primes. However, this is not the only "hard" problem in which we can base our security. In this section, we will introduce

1. The discrete logarithm problem.
2. The Diffie–Hellman key exchange protocol.
3. The ElGamal encryption scheme.

8.1 The discrete logarithm problem

In this section, we will present another computational problem that is believed to be hard. To do so, we first introduce the notion of *discrete logarithm*.

Let $\mathbb{G}$ be a cyclic group, with a generator g, written with multiplicative notation. Remember that this means that

$$\mathbb{G} = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}_{\geq 0}\},$$

that is, any element of $\mathbb{G}$ can be seen as a power of the generator g. We can also look at this from the other side: given any element $h \in \mathbb{G}$, there exists $n \in \mathbb{Z}_{\geq 0}$ such that

$$g^n = h.$$

This leads to the following definition.

Definition 8.1. *Let $\mathbb{G}$ be a cyclic group with generator g, written multiplicatively. Given $h \in \mathbb{G}$, we define the* discrete logarithm (DLog) *of h with respect to g as the value $n \in \mathbb{Z}_{\geq 0}$ such that $g^n = h$, and we denote it by*

$$\log_g h = n.$$

When the generator is fixed and there is no ambiguity, we might simply write $\log h$.

The name of the discrete logarithm comes from its similarity to logarithm as the inverse operation to exponentiation over the real numbers. That is, If $a, b \in \mathbb{R}$, and $c = a^b$, then we have that $\log_a c = b$.

In Sage, given a group element `h` and a generator `g`, the discrete logarithm of `h` with respect to `g` can be computed with `log(h,g)`.

Definition 8.2. *Let $\mathbb{G}$ be a cyclic group with generator g. The* discrete logarithm problem *relative to $\mathbb{G}$ consists of, given $\mathbb{G}, g$ and a uniformly random $h \in \mathbb{G}$, computing* $\log_g h$.

Similarly to the factorization problem, the discrete logarithm problem is believed to be hard (i.e. computationally infeasible) for some well-chosen groups. Again, we do not have a formal proof of the problem being hard, but it has been studied for decades, and no general algorithm faster than exponential-time has been found.

An important detail is the "well-chosen" part in the previous paragraph. That is, there exist some groups for which faster algorithms are known. Some cases can even be solved in time polynomial in the size of p. Consider, for example, $(\mathbb{Z}_p, +)$ for some large prime p, and a generator g. For this additive group, the discrete logarithm problem becomes, given $\mathbb{Z}_p, g$ and a uniformly random $h \in \mathbb{Z}_p$, to find x such that

$$gx \equiv h \pmod{p}.$$

But this can easily be solved as

$$x \equiv g^{-1}h \pmod{p},$$

where the inverse can be computed efficiently using the extended Euclidean algorithm. Therefore, these groups are not suitable for cryptographic purposes, if we want to rely on the discrete logarithm problem being hard.

A better candidate are the multiplicative groups $(\mathbb{Z}_n^*, \cdot)$ or, more precisely, a large subgroup of prime order. Without getting into much detail, the restriction to the prime-order subgroup is due to the Pohlig–Hellman attack,[1] which tells

[1] Pohlig, S., & Hellman, M. (1978). An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (corresp.). *IEEE Transactions on information Theory*, 24(1), 106-110.

us that the discrete logarithm problem in a composite-order group is as hard as the problem in the largest prime-order subgroup.

If n is prime, then the order of $\mathbb{Z}_n^*$ is $n-1$, and thus we want to ensure that the largest prime-order subgroup is as large as possible relative to n. This motivates the introduction of *safe primes*, which are prime numbers p such that $q = (p-1)/2$ is also a prime. This ensures that $\mathbb{Z}_p^*$ has order $2q$, and the subgroup of order q can be used.

To convince ourselves that looking for safe primes is efficient enough, let us try to find them with Sage, using the following code.

```
sec_param=128
while True:
    p = randint(2^(sec_param-1),2^(sec_param)-1)
    if p in Primes():
        q = (p-1)/2
        if q in Primes():
            print("p = "+str(p))
            print("q = "+str(q))
            break
```

Running on the free version of CoCalc, these are the approximate times to find a safe prime, for different choices of the security parameter

λ	Running time
128	Less than a second
256	A few seconds
512	About five minutes
1024	Two hours

This will be much faster with serious computing power (and a refined search algorithm), and nevertheless observe that this will be something that we only need to run once, since the prime can be reused without compromising the hardness of the problem.

Exercise 8.1. *If we want q as close to p as possible, why don't we look for primes p such that $q = p-1$ is also prime?*

Although, strictly speaking, no efficient algorithm is known, some algorithms that are better than exponential have been found for these groups, so this is not an ideal candidate either. The current record of broken discrete logarithm is in a group $\mathbb{Z}_p^*$ for a prime p of bitlength 795, which took around 3100 core-years.[2]

[2]Boudot, F., Gaudry, P., Guillevic, A., Heninger, N., Thomé, E., & Zimmermann, P.

Currently, the best choice is groups of points of elliptic curves. Elliptic curves are an advanced topic in mathematics, and lie at the intersection of algebraic geometry and number theory. We will not cover them in these notes, but it suffices to say that one can define a group law in the set of points of one such curve, and some of these curves are believed to have very hard discrete logarithms, much harder than the groups $\mathbb{Z}_n^*$ of the same size. In contrast with the discrete logarithm records in $\mathbb{Z}_n^*$, the largest known discrete logarithm solved corresponds to an elliptic curve of order n, for n a 114-bit integer. It took the researchers 13 days of parallel computation on 256 NVIDIA Tesla V100 GPUs.[3]

8.2 The Diffie-Hellman key exchange

In the first half of the course, we discussed symmetric cryptography. For two parties Alice and Bob to communicate using a symmetric encryption scheme, they need to first establish a shared secret key, in a process called *key agreement* or *key establishment*. This is a non-trivial task. Maybe they could meet in person and agree on a key, or maybe they could both trust a third party to handle the key agreement for them. But clearly this is not ideal, and depending on the context maybe not possible at all.

One way to solve this issue is to use an asymmetric encryption scheme as a *key encapsulation mechanism*: Alice chooses a random *symmetric key* k, and uses a public-key encryption scheme, like RSA, to encrypt the key and send it to Bob. Then Bob decrypts the message and learns k. They can do this because the public-key encryption scheme does not require sharing secret keys in advance. From this point onwards, Alice and Bob can use the key k to communicate using a symmetric encryption scheme, like AES.

One might ask why not use public-key encryption all the time, since it requires no shared keys. While this poses no security problem, asymmetric encryption schemes tend to be much less efficient that symmetric ones, so it is simply faster to establish a key using asymmetric encryption, and later use symmetric encryption.

An alternative approach to key encapsulation mechanisms is to use the following.

Definition 8.3. *A* key exchange protocol *is a procedure between two parties, at the end of which both parties know a common key.*

The first and best-known key exchange protocol is the Diffie–Hellman key exchange protocol, introduced in 1976,[4] and it works as follows. The only common input is a security parameter λ.

(2020, August). Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. In *Annual International Cryptology Conference* (pp. 62-91). Springer, Cham.

[3] https://github.com/JeanLucPons/Kangaroo.

[4] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6), 644-654.

1. On input λ, Alice chooses a uniformly random prime p of bitlength λ, and determines a cyclic group $\mathbb{G}$ of order p, and a generator g of $\mathbb{G}$.
2. Alice sends $(\mathbb{G}, g)$ to Bob.[5]
3. Alice chooses a uniformly random $a \in \mathbb{Z}_p$, computes $A = g^a$, and sends A to Bob. Similarly, Bob chooses a uniformly random $b \in \mathbb{Z}_p$, computes $B = g^b$, and sends B to Alice.
4. Now, Alice computes the key as $k = B^a$, and Bob computes the same key as $k = A^b$.

Since k is technically a group element, it is processed in some established way to obtain a bitstring, which is the actual key that will be used for symmetric encryption purposes.

The parameters $(\mathbb{G}, g)$ can be reused without compromising security, so steps (1) and (2) do not need to be run again every time that Alice and Bob want to share a key, but it is very important that the values a, b are always fresh.

Before discussing security, let us convince ourselves that indeed Alice and Bob end up with the same key. Observe that

$$B^a = \left(g^b\right)^a = g^{ab} = \left(g^a\right)^b = A^b.$$

Therefore, the value computed by each party is actually the same.

Notice how k was never sent from one side to the other. However, some partial information related to it was sent, so one might be worried that an eavesdropper might learn some information about the key from the intercepted values, A and B. We define the exact level of security that we want to attain.

Definition 8.4. *A key exchange protocol is* secure in the presence of an eavesdropper *if no efficient adversary that observes the protocol (that is, an adversary that sees $\mathbb{G}, g, A, B$) can tell the real key from a uniformly random bitstring of the same size.*

Notice that this is a very strong definition, which implies that not a single bit of the key is leaked.

So why is the Diffie–Hellman key exchange protocol secure? Consider the following scenario. The adversary eavesdrops A, B, and finds a by solving the discrete logarithm of A with respect to g. Then the adversary could simply compute B^a and learn the shared key. Therefore, to prevent such an attack, we must ensure that the discrete logarithm problem is hard in $\mathbb{G}$.

However, formally this is not enough, because conceivably an adversary could extract the key directly from A, B, without the need to solve any discrete logarithm. This motivates the introduction of the following related problem.

[5] Formally, some description of the group is published as part of the key. For example, if it has been agreed that the group is some $(\mathbb{Z}_p^*, \cdot)$, then it is enough to publish p.

Definition 8.5. *Let $\mathbb{G}$ be a cyclic group of primer order p, with generator g. Let a, b be uniformly random elements of $\mathbb{Z}_p$, and let*

$$A = g^a, \qquad B = g^b.$$

The computational Diffie–Hellman (CDH) problem *relative to $\mathbb{G}$ consists of, given $\mathbb{G}, g, A, B$, computing g^{ab}.*

If this problem is hard, then clearly an adversary will not be able to compute a Diffie–Hellman key from eavesdropping communications. However, our definition of security requires something stronger: that such a key cannot be distinguished from random strings.

Definition 8.6. *Let $\mathbb{G}$ be a cyclic group of primer order p, with generator g. Let a, b be uniformly random elements of $\mathbb{Z}_p$, and let*

$$A = g^a, \qquad B = g^b.$$

With probability $1/2$, let $C = g^{ab}$, otherwise let C be a uniformly random element of $\mathbb{G}$. The decisional Diffie–Hellman (DDH) problem *relative to $\mathbb{G}$ consists of, given $\mathbb{G}, g, A, B, C$, decide whether $C = g^{ab}$ or C is something else.*

Observe that, unlike any other computational problem that we have considered, the DDH problem can easily be solved with probability 1/2, by guessing at random. Thus, for decisional problems, we say that the problem is hard if there is no efficient algorithm that can do significantly better than that. For example, an efficient algorithm that succeeds in solving the DDH problem with probability 2/3 would be considered a breach of the problem.

Exercise 8.2. *Prove that:*

1. *If we can break the DLog problem, then we can break the CDH problem.*
2. *If we can break the CDH problem, then we can break the DDH problem.*

As is was the case with the factorization and RSA problems, there is no known algorithm that can solve CDH or DDH any faster than the DLog problem. Nevertheless, there is no formal proof that solving either of these allows us to solve DLog, so the problems are not known to be equivalent, hence why we require them for security of the Diffie–Hellman key exchange protocol.

Proposition 8.1. If the DDH problem is hard relative to a group $\mathbb{G}$, then the Diffie–Hellman key exchange, using the group $\mathbb{G}$, is secure in the presence of an eavesdropper.

8.3 The ElGamal encryption scheme

We introduce the ElGamal encryption scheme,[6] Unlike the RSA cryptosystem, the ElGamal encryption scheme works in a cyclic group of prime order. An advantage of this scheme is that it provides CPA security by default, without the need of padding, so no hash function is required.

- KeyGen: on input a security parameter λ, choose a cyclic group $\mathbb{G}$ of prime order p, and a generator g of $\mathbb{G}$. We will write $\mathbb{G}$ with multiplicative notation. Sample a uniformly random $x \in \mathbb{Z}_p$, and set $h = g^x$. Output the public key
$$\mathsf{pk} = (\mathbb{G}, g, h),$$
and the secret key
$$\mathsf{sk} = x.$$

- Enc: given a message $\mathsf{m} \in \mathbb{Z}_p$, with m small, and the receiver's public key $(\mathbb{G}, g, h)$, choose a uniformly random $r \in \mathbb{Z}_p$ and output the ciphertext
$$\mathsf{c} = (\mathsf{c}_1, \mathsf{c}_2) = (g^r, g^m h^r).$$

- Dec: given a ciphertext c and the secret key d, output
$$\log_g \frac{\mathsf{c}_2}{\mathsf{c}_1^x}.$$

It is easy to see that decryption recovers the original message encrypted. Indeed, observe that
$$g^m h^r = g^m (g^x)^r = g^{m+xr},$$
and thus
$$\log_g \frac{\mathsf{c}_2}{\mathsf{c}_1^x} = \log_g \frac{g^{m+xr}}{(g^r)^x} = \log_g g^m = m.$$

One thing that might seem counter-intuitive is the fact that we are supposed to find the discrete logarithm of g^m to recover the message. But, at the same time, we will require the DLog problem to be hard for security. The key point is that m is small relative to p, so that the DLog of g^m can be solved efficiently. Observe that this does not contradict the discrete logarithm problem, which states that the discrete logarithm should be hard to compute for *uniformly random* elements of $\mathbb{Z}_p$, but it is fine if it can be solved for small values.

Intuitively, the security of the scheme relies on the DLog problem being hard, because an adversary that can compute discrete logarithms would be able to recover x and run the decryption algorithm. Moreover, observe that the scheme

[6] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4), 469-472.

is *randomized*, that is, the same plaintext can produce different ciphertexts, depending on each encryption's randomness r.

Formally, again we require the DDH problem to be hard to ensure security.

Proposition 8.2. If the DDH problem is hard for a group $\mathbb{G}$, then the ElGamal encryption scheme in $\mathbb{G}$ is secure.

Below is an implementation of the ElGamal encryption scheme in $\mathbb{Z}_p^*$. The value of p used is a safe prime of bitlength 1024 found used the algorithm above.

```
### KEY GENERATION
# Choose parameters
p = 98477271628635149697160687227938079584387801057656524674547805684845362792314056005
q = (p-1)/2
# Check that p, q are primes
p in Primes(), q in Primes()
# Set the group as Z_n^*, choose a generator g and check that g has order q
G = Integers(p)
g = G(3)
g.multiplicative_order() == q
# Compute and output the keys.
x = randint(0,q)
h = g^x
pk = (p,g,h)
sk = x

### ENCRYPTION
# Choose a small message (so that its DLog can be computed)
m = 27593
if (m>=q):
    print("Message too large.")
else:
    # Sample randomness
    r = randint(0,q)
    # Compute the ciphertext
    c = (g^r, g^m*h^r)
    print(c)

### DECRYPTION
w = c[1]/(c[0]^x)
# Solve the discrete logarithm of w with respect to g by brute force
for m in range(q):
    if g^m == w:
        print(m)
        break
```

Chapter 9

Digital signatures

Part IV

Other topics

Chapter 10

Cryptanalysis

Appendix A

Ring theory

A ring is a slightly more complex algebraic structure, since it is equipped with two operations, the first of them with the exact same properties of a commutative group operation, whereas the second does not require the existence of inverse.

Definition A.1. *A* ring[1] *is a triple* $(\mathbb{K}, \circ, *)$*, where* $\mathbb{K}$ *is a set and* $\circ$ *and* $*$ *are operations on* $\mathbb{K}$*, that is, functions*

$$\begin{aligned} \circ: \ \mathbb{K}\times\mathbb{K} &\to \mathbb{K} & \qquad * : \ \mathbb{K}\times\mathbb{K} &\to \mathbb{K} \\ (x,y) &\mapsto x\circ y, & (x,y) &\mapsto x*y, \end{aligned}$$

which additionally satisfy the following properties:

1. $(\mathbb{K}, \circ)$ *is a commutative group.*
2. $(\mathbb{K}, *)$ *satisfies the following properties:*
    1. Associative law: $(x*y)*z = x*(y*z)$ *for all* $x, y, z \in \mathbb{K}$.
    2. Existence of identity: *there exists* $e \in \mathbb{K}$ *such that* $e*x = x*e = x$ *for all* $x \in \mathbb{K}$*. Such element* e *is called the* identity element *of* $*$.
    3. Commutativity: $x*y = y*x$ *for all* $x, y \in \mathbb{K}$.
3. Distributive law: $x*(y\circ z) = (x*y)\circ(x*z)$ *for all* $x, y, z \in \mathbb{K}$.*

Since we have two operations at the same time, we will adopt the additive and multiplicative notation from groups to represent each of them, respectively. That is, we will think of the first operation of a ring as a form of *addition* and

[1] In an abstract algebra context, the definition of a ring is more general, and what we are defining is known as a *commutative ring with unity*. Nevertheless, we stick to this definition for simplicity, since it is the only type of ring relevant to us.

the second as a form of *multiplication*. On input x, y, we write the result of the first operation by $x + y$, and the result of the second by xy. The identity elements of each operation are denoted by 0 and 1, respectively. The inverse of x with respect to the first operation is denoted by $-x$. The inverse of x with respect to the second operation, if exists, is denoted by x^{-1}. The following table summarizes the notation:

Operation	Operation on input x, y	Identity element	Inverse of x
$+$	$x + y$	0	$-x$
$\cdot$	xy	1	x^{-1}

We consider some examples:

- $(\mathbb{Z}, +, \cdot)$, with usual integer addition and multiplication, is a ring, since $(\mathbb{Z}, +)$ is a group with identity 0, $(\mathbb{Z}, \cdot)$ verifies associativity, commutativity and existence of identity (1), and it is easy to verify distributivity. Note, however, that $\mathbb{Z}$ does not contain multiplicative inverses, since for example there is no $x \in \mathbb{Z}$ such that $2x = 1$. For similar reasons, $(\mathbb{Z}_n, +, \cdot)$, with modular addition and multiplication, is a ring, for $n \in \mathbb{N}$.
- $(\mathbb{Q}[X], +, \cdot)$, where $\mathbb{Q}[X]$ is the set of polynomials with rational coefficients in variable X, $+$ is point-wise addition, and $\cdot$ is point-wise multiplication, is also a ring. The identity elements are the constant polynomials $p(X) = 0$ and $q(X) = 1$, respectively.

Consider the ring $\mathbb{Z}_9$, with addition and multiplication modulo 9. The following table gives the multiplicative inverses of each element:

x	0	1	2	3	4	5	6	7	8
x^{-1}	–	1	5	–	7	2	–	4	8

Note that some elements are not invertible, in this case 0, 3 and 6. Those elements in a ring that happen to have a multiplicative inverse receive a special name.

Definition A.2. *Let $\mathbb{K}$ be a ring. An element $x \in \mathbb{K}$ that has a multiplicative inverse is called a* unit. *We denote the set of units of $\mathbb{K}$ by $\mathbb{K}^*$.*

Note that the only thing that $(\mathbb{K}, \cdot)$ was missing to be a group is existence of inverses. By restricting ourselves to the subset $\mathbb{K}^*$ of invertible elements, we have that $(\mathbb{K}^*, \cdot)$ is a group. Note that, in the previous lesson, we defined $\mathbb{Z}_n^*$ to

be the set of invertible elements of $\mathbb{Z}_n$, so in this new formulation, we can state that $\mathbb{Z}_n^*$ is actually the set of units of $\mathbb{Z}_n$. Moreover, we now know that $\mathbb{Z}_n^*$ is a group with multiplication modulo n.

In light of the discussion above, we start this section by asking ourselves the following question.

Is it possible to have a ring $\mathbb{K}$ in which all the elements are invertible?

This will never be the case, unless the ring only contains one element, since the additive identity 0 cannot have a multiplicative inverse otherwise. To see this, assume that there exists $x \in \mathbb{K}$ such that $0 \cdot x = 1$. First,

$$0x = (1 + (-1))x = x + (-x) = 0,$$

using the distributive law and the properties of the multiplicative identity 1. Then we have that $1 = 0$. But then, this means that

$$x = 1x = 0x = 0,$$

using the properties of the multiplicative and additive identities. Thus, we conclude that every element is the same. And rings with just one element are not very interesting.

So, except for the trivial case, we know that 0 cannot have an inverse. What about the rest of the elements? In this case, the answer is affirmative: there exist rings in which every non-zero element is invertible, and we call those *fields*.

Definition A.3. *A* field *is a ring in which every non-zero element has a multiplicative inverse in the ring.*

Appendix B

Primality testing

Many modern cryptographic schemes require some very large prime numbers, so we are interested in generating these numbers efficiently. The basic strategy is very simple: pick a random number of the desired size, and check whether it is prime. If it is not, pick another. A consequence of the prime number theorem (Proposition 5.3) is that, on average, we need about λ tries to find a prime of bitlength λ, so that's not too bad.

But what about recognizing whether a number is prime or not? This part is solved with a *primality test*. In this section, we look at some of them.

The naive way to check primality is to check if the candidate integer $n = O(2^\lambda)$ is divisible by any other smaller integer. If that's not the case, then necessarily n is prime. So, in general, this algorithm runs in time $O(n)$, which is exponential in λ. We can do slightly better by observing that it is enough to check divisors up to $\sqrt{n}$.

Proposition B.1. Let $n \in \mathbb{N}$. If n is composite, then n has a non-trivial divisor $d \leq \sqrt{n}$.

Proof. We prove the result by contradiction. Assume that n is composite and has no non-trivial divisor smaller than $\sqrt{n}$. Since n is composite, it has at least two non-trivial divisors $a, b \in \mathbb{N}$, such that $ab = n$. But every divisor is larger than $\sqrt{n}$, therefore

$$n = ab > \sqrt{n} \cdot \sqrt{n} = n,$$

and thus $n > n$, which is a contradiction.

□

Still, our primality test would run in time $O(\sqrt{n})$, which is still exponential in λ. We need to look for a more efficient approach. We turn our attention to Fermat's little theorem:

Proposition B.2 (Fermat's little theorem)**.** Let p be a prime number. Then, for any $x \in \mathbb{Z}$ such that $p \nmid x$, we have that

$$x^{p-1} \equiv 1 \pmod{p}.$$

This theorem tells us about a condition that all prime numbers verify, which gives us an easy condition to test and discard composite numbers. Given a candidate n, choose some $x \in \mathbb{Z}$ such that $\gcd(n, x) = 1$, and compute

$$x^{n-1} \bmod n.$$

If the result is not 1, then we conclude that n is not a prime. This is known as the *Fermat primality test*, and it is very efficient. But what happens if the result is 1? Does this mean that n is a prime? Unfortunately, it is not as simple as this. For example, take $n = 91$ and $x = 3$. It is easy to verify that

$$3^{90} \pmod{91} = 1,$$

but $91 = 7 \cdot 13$, so it is not a prime. We call the numbers that produce these "false positives" *pseudoprimes*.

Definition B.1. *Let $n \in \mathbb{Z}$ be a composite number, and let $x \in \mathbb{Z}$ such that $\gcd(x, n) = 1$. We call n an* x-Fermat pseudoprime *if*

$$x^{n-1} \equiv 1 \pmod{n}.$$

Moreover, for any x there are many x-Fermat pseudoprimes. Okay, so everybody don't panic. Fermat's little theorem tell us that primes verify the condition

$$x^{p-1} \equiv 1 \pmod{p}$$

for *every* x such that $\gcd(p, x) = 1$. So surely we can find some other base x so that 91 cannot fool the test. Indeed,

$$5^{90} \bmod 91 = 64.$$

So that's it, we are now sure that 91 is not a prime, because it does not pass the test for $x = 5$. Problem solved.

Or is it? What if there are some truly evil numbers that can fool the Fermat test for all the possible bases?

Definition B.2. *Let $n \in \mathbb{Z}$ be a composite number. We say that n is a* Carmichael number *if it is a x-Fermat pseudoprime for every $x \in \mathbb{Z}$ such that $\gcd(n, x) = 1$.*

Unfortunately, there are too many of these Carmichael numbers. For large values of $B \in \mathbb{N}$, the number of Carmichael numbers up to B is approximately $B^{2/7}$. This means that a significant amount of numbers will fool our test, even if we run it for all the possible bases. We need a better test.

The solution lies on a strengthened version of Fermat's little theorem.

Proposition B.3. Let $p \in \mathbb{N}$ be an odd prime, and let $p - 1 = 2^s t$ such that $2 \nmid t$. If $\gcd(p, x) = 1$, then either

$$x^t \equiv 1 \pmod{p},$$

or there exists $i \in \{0, 1, \ldots, s-1\}$ such that

$$x^{2^i t} \equiv -1 \pmod{p}.$$

Again, the idea is to test our numbers against this result, and see if they satisfy the equations. This version is called the *strong Fermat primality test*. Observe that, in the worst case, we need to perform s checks, and if p has bitlength λ, then $s = O(\lambda)$, and each check amounts to modular exponentiation, so overall this is efficient. As before, this new test also produces false positives.

Definition B.3. *Let $n \in \mathbb{Z}$ be an odd composite integer, and let $n - 1 = 2^s t$. Let $x \in \mathbb{Z}$ such that $\gcd(x, n) = 1$. We call n a* strong x-Fermat pseudoprime *if*

$$x^{t-1} \equiv 1 \pmod{n},$$

or there exists $i \in \{0, 1, \ldots, s-1\}$ such that

$$x^{2^i t} \equiv -1 \pmod{n}.$$

Exercise B.1. *Check that* 2047 *is a strong* 2*-Fermat pseudoprime, because it satisfies the first condition, and that* 91 *is a strong* 10*-Fermat pseudoprime, because it satisfies the second condition.*

So why bother with the strong Fermat test, if it has the same flaw? The key point is that, even if we have strong pseudoprimes, the strong Fermat test does not have its version of Carmichael numbers. That is, for any composite number n we will always be able to find a base such that n does not pass the strong test, showing that it is indeed composite. Moreover, most of the bases will do!

Proposition B.4 (Monier–Rabin)**.** Let $n > 9$ be an odd composite integer. Then, the number of bases x smaller than n such that n is a strong x-Fermat pseudoprime is at most $\frac{1}{4}\varphi(n)$.

This is a very strong result. Since $\varphi(n) < n$, this tells us that, by picking a base in $\mathbb{Z}_n$ at random, there is only a probability of $1/4$ that the test lies. Of course, we want a smaller probability, so we repeat the test many times. By using λ iterations for different random bases, we bring the error probability down to $1/4^\lambda$. Observe that this decreases exponentially in λ! To give some concrete numbers, for $\lambda = 1024$, we have that

$$\frac{1}{4^\lambda} \approx 3.094346 \cdot 10^{-67},$$

and this looks like a failure probability that we can live with.

Asymptotically, we have an algorithm that runs λ iterations, and each of these is computing $O(\lambda)$ exponentiations, so in total we have a running cost of $O(\lambda^2)$ modular exponentiations.

This test is known as the *Miller–Rabin primality test*, and it is in essence what is used in practice to check for primality, due to its high efficiency and almost-perfect reliability.

If you are still concerned about the error probability, there are some alternatives that *never* produce erroneous results, while still running in polynomial time. However, they are much slower than the Miller–Rabin test, which is why they are not often used in practice.[1]

[1] Agrawal, M., Kayal, N., & Saxena, N. (2004). PRIMES is in P. *Annals of mathematics*, 781-793.

Appendix C

Refreshers

C.1 Set notation

A *set* is a well-defined collection of objects. Such objects are said to be *elements* of the set, or that they *belong* to the set. For example, the set of the vowels is

$$V = \{\mathrm{a}, \mathrm{e}, \mathrm{i}, \mathrm{o}, \mathrm{u}\}.$$

In the above line we are giving a name to the set, V, and we are specifying the list of its elements: a, e, i, o and u. When describing a set explicitly, we write the list of its elements between braces { }.

Two sets are equal if they have exactly the same elements. An element cannot belong 'twice' to a set. Therefore, we can say that

$$V = \{\mathrm{a}, \mathrm{e}, \mathrm{i}, \mathrm{o}, \mathrm{u}\} = \{\mathrm{u}, \mathrm{o}, \mathrm{i}, \mathrm{e}, \mathrm{a}\} = \{\mathrm{a}, \mathrm{a}, \mathrm{e}, \mathrm{e}, \mathrm{e}, \mathrm{i}, \mathrm{o}, \mathrm{u}\}.$$

The symbol $\in$ indicates membership of an element in a set. For example, we can write $\mathrm{a} \in V$, because a belongs to the set V. On the other hand, we have that $\mathrm{b} \notin V$, since b is not any of the elements of V.

There are some number sets that show up very frequently, so we give them special names.

- $\mathbb{N}$: set of natural numbers.
- $\mathbb{Z}$: set of integer numbers.
- $\mathbb{Q}$: set of rational numbers.
- $\mathbb{R}$: set of real numbers.
- $\mathbb{C}$: set of complex numbers.

Observe that, unlike in the prior examples, all these sets are *infinite*, that is, they have an infinite number of elements. Obviously we cannot describe an infinite set explicitly, as we have done with the set of vowels. What we can do is refer to other sets that we have already defined and define restrictions on them. For example, we can define the set of even natural numbers as the set of natural numbers that are multiples of 2. Formally, we write this set as

$$\{n \in \mathbb{N} \mid n = 2k \text{ for some } k \in \mathbb{N}\}.$$

Here we have introduced some new notation. Instead of explicitly enumerating all the elements of a set, we give some conditions. We read the description above as 'the set of elements of the form indicated on the left of the vertical line, such that they verify the condition on the right'. In this case, the set of natural numbers such that they are of the form $2k$ for some natural value of k. Similarly, we can define the set of all real numbers greater than 5 in the following way:

$$\{x \in \mathbb{R} \mid x > 5\}.$$

We denote the size (number of elements) of a set S by $\#S$.

We can produce new sets by considering the *product* of known sets: given two sets S, T, we define the set $S \times T$ as the set whose elements are the pairs (s, t), where $s \in S$ and $t \in T$. For example,

$$\{0,1\} \times \{0,1,2\} = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}.$$

Observe that $\#(X \times Y) = \#X \cdot \#Y$. It is easy to generalize this definition to products of three or more sets. In particular, given a set S, we define

$$S^n = \underbrace{S \times S \times \cdots \times S}_{n \text{ times}}$$

In this course, we will often use the set $\{0,1\}$ of possible bits, the set $\{0,1\}^\ell$ of possible bitstrings of length ℓ, and the set $\{0,1\}^*$ of bitstrings of any length. Observe that

$$\#\{0,1\} = 2, \qquad \#\{0,1\}^\ell = 2^\ell, \qquad \#\{0,1\}^* = \infty.$$

Exercise C.1. *Write these sets using implicit notation:*

- *The set of complex numbers with real part equal to* 1*.*
- *The set of pairs, where the first component of the pair is a rational number and the second component is an odd natural number.*
- *The set of bitstrings of length* 10 *with exactly* 5 *zeros.*

C.2 Probability theory

We will deal with probability distributions over finite sets. In particular, recall that the *uniform distribution* over a set S is the probability distribution that assigns the same probability $1/\#S$ to each element of S. We denote sampling an element x from the uniform distribution over S by

$$x \leftarrow S.$$

For example, the notation

$$\mathbf{b} \leftarrow \{0,1\}^{128}$$

means that $\mathbf{b}$ is a uniformly random bitstring of length 128.

Given an event A, we denote the *probability of* A by $\Pr[A]$. Given two events A, B, we denote the *probability of* A *conditioned on* B by $\Pr[A|B]$, and if $\Pr[B] \neq 0$ we have that

$$\Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]},$$

where $\Pr[A \cap B]$ means the probability of both A and B happening. Recall that, if A and B are independent events, then

$$\Pr[A \cap B] = \Pr[A] \cdot \Pr[B].$$

Exercise C.2. *Compute the probability of a random bitstring of length* 4 *being the string* 1110.

C.3 Asymptotic notation

Asymptotic notation allows us to easily express the *asymptotic behaviour* of functions, that is, how the function changes for arbitrarily large inputs, with respect to some other function. For example, take the functions defined by

$$f(x) = x, \qquad g(x) = x^2.$$

Both tend to infinity as x tends to infinity, but the second does it "faster". More precisely, let

$$f, g : \mathbb{N} \to \mathbb{N}$$

be two functions. We write

$$f(x) = O(g(x))$$

when there is some $N, M \in \mathbb{N}$ such that, for all $x > N$, we have

$$f(x) \leq M \cdot g(x).$$

We read this as "f is big-O of g". Then, back to the initial example, we can say write

$$x = O(x^2).$$

Note that, because the big-O notation "absorbs" constants into M, we can write

$$2x = O(x),$$

even though $2x \geq x$ for $x \in \mathbb{N}$.

Big-O notation is useful for representing bounds on the growth speed of a function. By saying, for example, that a function f satisfies

$$f(x) = O(x^3),$$

we are saying that, at worst, the function f grows as fast as a cubic polynomial. Therefore, in particular, it will not grow as fast as a polynomial of degree 4, or an exponential function like 2^x.

We recall that logarithmic functions grow slower than polynomials of any degree, and polynomials of any degree grow slower than exponential functions. Given two polynomials of different degrees, the one with the higher degree grows faster.

Exercise C.3. *Decide whether each of these statements is true or false.*

- $10^{10}x^3 = O(x^4)$.
- $10^x = O(x^4)$.
- $\log(x) = O(x \log x)$.
- $4^x = O(2^x)$.

C.4 Polynomial division

Consider two polynomials

$$A(X) = a_k X^k + a_{k-1} X^{k-1} + \cdots + a_1 X + a_0,$$
$$B(X) = b_\ell X^\ell + b_{\ell-1} X^{\ell-1} + \cdots + b_1 X + b_0,$$

where $k \geq \ell$. Then, we have the following result.

Proposition C.1. Let $A(X)$ and $B(X)$ be the polynomials defined above. Then, there exist polynomials $Q(X)$ and $R(X)$ such that

$$A(X) = B(X)Q(X) + R(X),$$

where the degree of R is smaller than ℓ. In this case, Q is called the *quotient* and R is called the *remainder* of the division.

The algorithm is very similar to the algorithm of integer division. The idea is to try to find factors such that, when multiplied by $B(X)$, allow us to remove the highest-degree term left in $A(X)$, and use these terms to build $Q(X)$. Although very simple, the idea is cumbersome to explain for general polynomials, so we illustrate it with an example. Let

$$A(X) = 3X^5 + X^4 + 2X^2 + 7, \qquad B(X) = X^3 + X^2 + X.$$

We arrange them in the usual diagram:

$$\begin{array}{llll|l} 3X^5 & +x^4 & +2x^2 & +7 & X^3 + X^2 + X \end{array}$$

We want to remove $3X^5$, so we try to find a factor $f(X)$ such that $f(X)X^3 = 3X^5$. Thus, we choose $f(X) = 3X^2$, multiply it by $B(X)$, and subtract the result from $A(X)$, obtaining a lower-degree polynomial:

$$\begin{array}{llll|l} 3X^5 & +X^4 & +2X^2 & +7 & X^3 + X^2 + X \\ -2X^4 & -3X^3 & +2X^2 & +7 & 3X^2 \end{array}$$

We now look at the new polynomial, $-2X^4 - 3X^3 + 2X^2 + 7$, and again try to remove the highest-degree monomial, which we achieve by multiplying X^3 by $-2X$.

$$\begin{array}{llll|l} 3X^5 & +X^4 & +2X^2 & +7 & X^3 + X^2 + X \\ -2X^4 & -3X^3 & +2X^2 & +7 & 3X^2 - 2X \\ -X^3 + 4X^2 & & +7 & & \end{array}$$

Again, we want to remove the term $-X^3$, so we multiply $B(X)$ by -1:

$$\begin{array}{llll|l} 3X^5 & +X^4 & +2X^2 & +7 & X^3 + X^2 + X \\ -2X^4 & -3X^3 & +2X^2 & +7 & 3X^2 - 2X - 1 \\ -X^3 + 4X^2 & & +7 & & \\ 5X^2 & +X & +7 & & \end{array}$$

Since the degree of the current dividend is smaller than the degree of the divisor, we are done. We conclude that the quotient of the division of $A(X)$ by $B(X)$ is

$$3X^2 - 2X - 1,$$

and the remainder is

$$5X^2 + X + 7.$$

Note that the above example works in $\mathbb{Q}$, but in general operations on the coefficients must take into account which field we are in. For example, if our coefficients are in $\mathbb{F}_5$, we cannot "divide" by 3, but we can find the inverse of 3 modulo 5, and we must ensure that every coefficient is reduced modulo 5.