CRITTOGRAFIA

*Book Series*

4

# CRITTOGRAFIA

*Book Series*

*It is impossible to agree beforehand about things*
*of which one cannot be aware before they happen*

— Polibyus (150 BC)

La collana raccoglie le opere scientifiche che riguardano e approfondiscono l'affascinante, enigmatico e complesso campo crittografico.
La Crittografia è una materia molto ampia, che comprende tanto la progettazione di algoritmi, quanto lo sviluppo di tecniche crittoanalitiche. L'intento è quello di raccogliere opere che presentino e analizzino sia gli aspetti più teorici, tra cui le basi matematiche, sia quelli più pratici, tra cui gli aspetti protocollari. In questa ottica, inoltre, è interessante e necessario fornire visibilità alle innovazioni più promettenti, come la crittografia *postquantum*, la tecnologia blockchain e la cifratura nel cloud.
La collana ospita volumi che trattano ogni ambito della Crittografia, interessando e raggiungendo trasversalmente differenti contesti scientifici e divulgativi: note di lezioni universitarie per favorire la comprensione e la diffusione di tale disciplina; atti di convegni specializzati, per incrementare la consapevolezza della comunità scientifica nazionale e internazionale; monografie, che comprendono anche tesi di laurea e di dottorato, per divulgare ricerche e sperimentazioni.

The book series collects cryptographic works with ample scope.
Cryptography is a wide discipline, encompassing algorithm design and the investigation of cryptanalytic techniques. The book series aims at presenting both theoretical aspects, in particular the mathematical bases, and practical aspects, e.g. protocols. Along this line, we want to highlight the most promising innovations, such as *postquantum* cryptography, blockchain technology and cloud encryption.
The book series hosts lecture notes, to help spreading the knowledge of this fascinating subject, as well as workshop proceedings, to help the Italian scientific community collaborate, as well as specialized monographs, including Master's theses and PHD theses.

MICHELA CERIA
GIANCARLO RINALDO
MASSIMILIANO SALA

# BITS, BYTES AND FRIENDS

aracne



ISBN
979–12–5994–079–7

FIRST EDITION
ROMA 5 JANUARY 2022

# Contents

# Preface

The national initiative "De Componendis Cifris" aims at fostering the teaching and the research of cryptography in Italy, including its applicative aspects. Under the guidance of the late Michele Elia, we have started several publishing projects. This book in your hands is the fourth volume of our first book series, "Crittografia".

This book, titled *Bits, Bytes and Friends* is a contribution that tries to fill a gap in the teaching of cryptography at university level in courses for non-mathematicians.

Indeed, when cryptography is taught to students in Computer Science or Engineering, the mathematical part is often omitted, because the background of the students would not allow for a complete exposition of these aspects. We are very pleased to see a growth in lecturing of cryptographic courses and we have therefore prepared this booklet in the hope it would help students to understand the core mathematical part without the need of an extensive algebraic background.

# Introduction

Since 2003 Prof. Massimiliano Sala has been lecturing undergraduate and graduate courses in Coding Theory and Cryptography. Prof. Giancarlo Rinaldo and Dr. Michela Ceria have been involved in several courses with Prof. Sala. The students have been mainly from Mathematics, Computer Science and Engineering. While mathematical notions are not strictly required to implement cryptographic primitives and protocols, the student that wants to understand the inner working of a modern cryptosystem needs at least some notions of Discrete Mathematics and Algebra. In this book we present the material that has been used for more than a decade in these courses, which was specifically developed for students coming from a Computer Science / Engineering background. Therefore, what is presented here is the essential theoretical part that the three authors found useful in their courses.

The book starts with introducing the basic concept of a *bit*, both from an algebraic point of view and a practical view. Then the book describes other structures that can be constructed starting from bits: polynomials, vectors and multivariate polynomials.

In the second chapter *bytes* are introduced, with special care taken in the comparison between their formal algebraic definition and their actual use in Computer Science. The concept of (vectorial) Boolean functions is explained, which represent a formal algebraic description of algorithms generating bits. In other words, any time an algorithm needs bits in input and output, it is actually computing a Boolean function.

In the third chapter the book deals with algebraic concepts which are very close to those employed in bytes, and therefore we used the title *friends*. In particular, we present some elementary properties of numbers and primes, which are useful in public-key cryptography. Indeed, a cryptosystem is secure only if there is an underlying mathematical problem which is difficult to solve. Number Theory offers many examples of such problems, such as integer factorization.

The final chapter outlines a few cryptosystems, for the sake of exposition, linking them to the previous chapters. Although this book is not about cryptography, these cryptosystems may serve as a motivation for the curious readers.

Since this book is aimed at students unfamiliar with most abstract mathematics, its expository style is elementary, full of examples and simple applications, with lots of exercises that will help the reader to assess his/her progress.

An interested reader can continue to study with [5, 1, 2].

Chapter I

# Bits standard operations and logic

## 1.1. Preliminaries

A *bit* (binary digit) is a unit of measure for information, introduced by C. Shannon in 1948. We may view a bit as the minimal amount of information needed in order to distinguish among two events occurring with the same probability.

Bits are used in Information Theory and, in general, in most of Computer Science applications. They are denoted with the constants $0$ and $1$, representing the two events with the same probability. Their set is often denoted with $\{0,1\}$, but we need another notation, that is,

$$\mathbb{F}_2 = \{0,1\}\,.$$

With this notation we mean that we can perform operations on bits. More precisely, we want to introduce two operations, *sum* and *multiplication*, retaining some similarity with the usual operations of sum and product for *numbers*. The numbers we are interested in are *integers*, which we collect in a set called $\mathbb{Z} = \{\ldots,-1,0,1,2,\ldots\}$, *non-negative integers* (sometimes called *natural numbers*), which we collect in a set called $\mathbb{N} = \{0,1,2,3,\ldots\}$, and *rational numbers*, which we collect in a set called $\mathbb{Q} = \{\ldots,-11,\frac{-5}{101},0,\frac{1}{2},3,\ldots\}$.

Since $\mathbb{F}_2$ is so small, we can use the following table to show how to sum and multiply bits. The first column and the second contain the values of two input variables, $a$ and $b$, representing the two bits we sum or multiply; the third and the fourth, respectively, contain the sum and the product of $a$ and $b$.

| $a$ | $b$ | $a+b$ | $a\cdot b$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 |

**Table 1.1.** Sum and product

**Exercise 1.** *Compute the following operations in* $\mathbb{F}_2$*:*

— $(1+1)+0$
— $(1+1)+1$
— $(1+1)\cdot 1$
— $(0+0)+1+(1+0)\cdot 1$

Operations on bits share properties with those involving integer or rational numbers, as we are going to see in the following, starting with a comparison between the sum in $\mathbb{F}_2$ and the sum in $\mathbb{Z}$.

We can sum $2, 3$ and $4$ in $\mathbb{Z}$ and it happens that

$$(2+3)+4 = 5+4 = 9 = 2+7 = 2+(3+4),$$

so we can write also $9 = 2+3+4$, omitting the parentheses. This holds for any three numbers in $\mathbb{Z}$.

We claim that this holds *also* for the sum of bits. For example

$$(1+0)+1 = 1+1 = 0 = 1+(0+1) = 1+0+1\,.$$

The reader can verify our claim for any $a, b, c \in \mathbb{F}_2$.
Any time we have a set and a sum operation which satisfies the general property

$$\forall a, b, c, \quad (a+b)+c \;=\; a+(b+c) \;=\; a+b+c\,,$$

we say that the operation is *associative*.

Therefore, we can conclude that both the sum in $\mathbb{Z}$ and the sum in $\mathbb{F}_2$ are associative operations.

Consider now $2, 3 \in \mathbb{Z}$. We know that $2+3 = 3+2 = 5$ and this holds for any pair of integers. We claim that this holds also for bits, as for example

$$0+1 \;=\; 1+0 \;=\; 1\,.$$

We leave to the reader the verification of this statement for each $a, b \in \mathbb{F}_2$.

We can formalize this property by saying that both the sum in $\mathbb{Z}$ and the sum in $\mathbb{F}_2$ are *commutative* operations. In a more general setting, a sum operation on a set is called commutative if for any $a, b$ in that set we have

$$a + b = b + a\,.$$

**Exercise 2.** *Compute the following operations*

— $a = 1+1+1+0+0+0+0+1$
— $b = 1+1+1+1+0+0+0+0$

*May you deduce b once knowing a? If so, which properties of bits are you using?*

Now we take a close look at $0 \in \mathbb{Z}$. Considering any integer $a$, we have that $a + 0 = 0 + a = a$, as for example $3 + 0 = 0 + 3 = 3$. In other words, summing a number with zero leaves the number unchanged (and this happens *only* for $0$).

The same happens with $0 \in \mathbb{F}_2$, since $0+0 = 0$ and $0+1 = 1+0 = 1$. In a general setting, if we have a sum operation with a special element $e$ such that $a + e = e + a = a$ for any $a$ in the set, then we say that $e$ is the *neutral element* of the operation.

Therefore, we can say that $0 \in \mathbb{F}_2$ is the neutral element of the sum in $\mathbb{F}_2$, while $0 \in \mathbb{Z}$ is the neutral element in $\mathbb{Z}$.

**Remark 3.** *When there is a set with a sum operation, it is usual to call "0" the neutral element. This is unfortunate because for example the $0 \in \mathbb{F}_2$ and the $0 \in \mathbb{Z}$ are two totally different objects. We are confident that the readers will soon be accustomed to this abuse of notation.*

Another important property of the sum in $\mathbb{Z}$ is that, given an element $a \in \mathbb{Z}$, we can always find an element $b \in \mathbb{Z}$ such that $a + b = b + a = 0$. For example, if $a = 3$, we need $b = -3$ to get $3 + (-3) = (-3) + 3 = 0$.

In the general case, when there is a set with a sum, if for any element $a$ there is another element $b$ such that $a + b = 0$ (and this