Notes on Data Encryption

Riccardo Lo Iacono

January 27, 2026

Document is WIP, typos could be found

Contents.

- 1 - Introduction.

Data encryption dials with how informations, see [1] for the definition, can be transmited securely through a channel.

More in details, if m is a message we want to send through a channel, first we have to encode it in a form that allows it to be transmited; then we want that such message is meaningless to those who have no right to read it. On the other hand, we want to be able to retrieve the message once this is recived.

To achive the above two disciplines were found: Cryptography and Code theory; the former focuses on how to make data secure, the latter provides methods to transmit data through a channel.

- 1.1 - About these notes.

These notes will focus on both Cryptography and Code theory, or at least, some parts of them.

More precisely, we begin by introducing some fundamental concepts of abstract algebra and projective geometry, we then discuss what public key encryption is focusing on the RSA and the ElGamal algorithm; we continue with describing some algorithms to factor integers, and conclude with several types of codes.

The following notation will be used throughout the document.

- $\mathcal{A}, \mathcal{B}$ and $\mathcal{E}$ will indicate, respectively, the sender, the reciever and an unauthorized individual attempting to capt our message.
- $\mathcal{C}$ will denote codes.
- Words in a code $\mathcal{C}$ will be represented by $\mathbf{w}$, with the occasional use of subscripts.

Any other symbol will be explained beforehand.

- 2 - Mathematical background.

In this section we provide the reader with some notions of abstract algebra; we recall what Greatest Common Divisor (GCD) and Least Common Multiple (LCM) are, we discuss congruence modulo n, and present groups and rings, and discuss some well know results on them.

Also, some broad concepts of projective geometry will be given; we focus on what projective space is, what the sum of projective points looks like, and to conclude, we give consider elliptic curves.

- 2.1 - Some abstract algebra.

In what follows, we assume the reader to have a basic understanding of number sets and equivalence relations.

Definition (Divisibility) Let $a, b \in \mathbb{Z}$. We say that a divides b, and write $a|b$, if

$$\exists q \in \mathbb{Z} \text{ s.t. } b = qa.$$

Otherwise we say that a does not divide b, and write $a \nmid b$.

Divisibility allows us to define two important concepts: LCM and GCD.

Definition (LCM) Let $a, b \in \mathbb{Z}$. Let $m \in \mathbb{Z}$. We say that m is the LCM for a and b if, the following holds:

1. $a|m$ and $b|m$, and
2. If $\exists m' \in \mathbb{Z}$ such that $a|m'$ and $b|m'$, then $m|m'$.

Definition (GCD) Let $a, b \in \mathbb{Z}$. Let $d \in \mathbb{Z}$. We say that d is the GCD for a and b if, the following holds:

1. $d|a$ and $d|b$, and
2. If $\exists d' \in \mathbb{Z}$ such that $d'|a$ and $d'|b$, then $d'|d$.

The computation of the GCD is done by the euclidean algorithm; we present an efficient inpementation of it in *Section* **??**.

ToDo. Add label in section 4.

Definition (Congruence modulo n) Let $a, b \in \mathbb{Z}$, and let $n \in \mathbb{Z}$ be a fixed integer. We say that a is congruent b modulo n, and write $a \equiv b \pmod{n}$ if and only if

$$\exists k \in \mathbb{Z} \text{ s.t. } a = kn + b.$$

- 2.1.1 - A brief introduction to groups.

Definition (Group) Let G be a set. Assume $\cdot : G \to G$ to be some function. We say that the pair $(G, \cdot)$, often simply as G, is a group if the following properties hold:

- $\forall a, b, c \in G, a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- $\exists e \in G \; \forall g \in G$ s.t. $g \cdot e = e \cdot g = g$;
- $\forall g \in G \; \exists g^{-1} \in G$ s.t. $g \cdot g^{-1} = g^{-1} \cdot g = e$.

If it also holds that $\forall a, b \in G, a \cdot b = b \cdot a$, we say that G is an abelian (or commutative) group.

We consider finite groups: that is, group with finitely many elements. Precisely, we are interested on the following class of groups.

Definition (Cyclic group) Let G be a group, and let $g \in G$. Denote by g^k the application of $\cdot$ on g, k times. Denote by $\langle g \rangle$ the set of all powers of g. We say that G is cyclic if $\langle g \rangle = G$.

Definition (Subgroup) Let G be a group, and let $H \subseteq G$. We say that H is a subgroup of G, if H is a group under the operation inherited from G.

Theorem (Langrange's) *Let G be a group, and let H be one of its subgroups. Let $\mathrm{Ord}(G), \mathrm{Ord}(H)$ denote the order (the number of elements) of G and H, respectively. Then, it holds*

$$\mathrm{Ord}(H) | \, \mathrm{Ord}(G).$$

When the group in question is cyclic, Langrange's theorem can be states as follow: let $g \in G$ and denote by $\mathrm{Ord}(g)$ the smallest integer n such that $g^n = 1$, then, it holds $\mathrm{Ord}(g) | \, \mathrm{Ord}(G)$.

We will implicitely use Langrange's theorem when we discuss RSA and ElGamal algorithms.

- 2.1.2 - A brief introduction to rings.

Definition (Ring) Let R be a a set, and let $+, \cdot$ be two binary operations on R. We say that the triplet $(R, +, \cdot)$, often as R, is a ring if and only if the following conditions hold.

1. For all $a, b \in R, a + b = b + a$.
2. $a + (b + c) = (a + b) + c, \forall a, b, c, \in R$.

3. There exist a neutral element for $+$; that is, $\exists 0 \in R$ s.t. $a + 0 = a, \forall a \in R$.
4. Each element has an additive oppposite, i.e., $\forall a \in R, \exists -a \in R$ such that $a + (-a) = (-a) + a = 0$.
5. $\cdot$ is associative; that is, $a(bc) = (ab)c, \forall a, b, c \in R$.
6. For all $a, b, c \in R, a(b + c) = ab + ac$.

Definition (Unital ring) Let $(R, +, \cdot)$ be a ring. We say that R is a unital ring, or a ring with unity, if there exists $1 \in R$ such that $1 \neq 0$ and $1a = a1 = a, \forall a \in R$.

Definition (Abelian ring) Let $(R, +, \cdot)$ be a ring. If for all $a, b \in R$ it holds that $ab = ba$; R is called commutative, or abelian, ring.

Definition (Integral domain) Let $(R, +, \cdot)$ be a commutative ring. If, for all $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$; we say that R is an integral domain.

Definition (Division ring) Let $(R, +, \cdot)$ be a unital ring. We say that R is a division ring if, for all $a \in R$ exists a unique $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Definition. Let $(R, +, \cdot)$ be a ring. We say that R is a field, if and only if R is a commutative division ring.

In the following we denote fields with $\mathbb{F}$, while Galois fields, i.e., fields with finitely many elements, with $\mathrm{GF}(q)$ where q is the number of elements in the fields.

In *Section* **??** we discuss several codes, most of which make use of polynomial. In this context, an issue may occur: the chosen polynomial has no solution within the field in use. To solve it, we make use of field extensions, which are formally defined below.

Definition. Let $\mathbb{F}$ be a field. Denote by $\mathbb{F}[x]$ the set of polynomials with coefficients in $\mathbb{F}$[1]. Let $f(x) \in \mathbb{F}[x]$ be a irreducible polynomial, i.e., a polynomial with no solution[2]. We call field extension a field $\mathbb{F}'[x]$ in which we impose the existence of a solution for $f(x)$. That is,

$$\mathbb{F}'[x] = \{a + bi \mid a, b \in \mathbb{F} \text{ and } i \text{ root for } f(x)\}.$$

[1] It can be proved that $\mathbb{F}[x]$ is also a field.

[2] To be more precise a polynomial with no solution is garanteed to be irreducible if its degree is at most 3.

- 2.2 - Notions of projective geometry.

In what follows we assume that notions such as points, lines, planes in the geometrical sense, in addition to the notion of vector spaces are known to the reader.

Definition (Ray) Let $\mathbb{F}$ be a field, and let $\mathcal{V}$ be a vector space over $\mathbb{F}$. Let $\mathbf{v} \in \mathcal{V}$ be non-zero. We call the set

$$[\mathbf{v}] = \{k\mathbf{v} \mid k \in \mathbb{F}^*\}$$

a ray.

Definition (Projective plane) Let $\mathbb{F}$ be a field and let $\mathcal{V}$ be a vector space over F. Let $\mathrm{Dim}(\mathcal{V}) = 3$. We define the projective plane $\mathbb{P}^2$ as the set of rays of V. An element $X \in \mathbb{P}^2$ is called a point.

In our discussion we usually consider projective points in *homogeneous* coordinates; that is, if $X = [x : y : z]$ is a projective point at least one of the x, y, z is non-zero.

The relation with ordinary plane geometry is done as follow:

- Any point $(x, y) \in \mathbb{R}^2$ becomes a projective point $[x : y : 1]$; and
- Any point $[x : y : 0] \in \mathbb{P}^2$, which do not belong to Euclidean geometry, are called point at infinity.

We now present *elliptic curves* which are the main reason we discuss projective geometry.

Definition (Elliptic curves) Let $\mathcal{V}$ be a vector over some field $\mathbb{F}$. An elliptic curve $\mathcal{C}$ is the set of points of $\mathbb{P}^2$, that are solution to an equation of the form

$$y^2 = x^3 + ax + b.$$

In our treating, we consider non-singular elliptic curves; that is, such that the discriminant is non zero, i.e., $\Delta = -16(4a^3 + 27b \neq 0)$.

References.

[1] Claude E. Shannon. “A mathematical theory of communication”. In: *Bell Syst. Tech. J.* 27.3 (1948), pp. 379–423. DOI: 10.1002/J.1538-7305.1948.TB01338.X.

Acronyms.

GCD Greatest Common Divisor. 2

LCM Least Common Multiple. 2