Notes on Data Encryption

Riccardo Lo Iacono

January 29, 2026

Document is WIP, typos could be found

Contents.

- 1 - Introduction.

Data encryption dials with how informations, see [3] 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 $\langle g \rangle = G$.

- 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,

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

- 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.

[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.

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 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, and we denote them as $\mathcal{O}$.

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

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

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

with $a, b \in \mathbb{F}$.

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

In *Section* **??** we treat the ElGamal algorithm by means of elliptic curves; in this context given $\mathcal{C}$ an elliptic curve, we are required to compute the sum of two point $P, Q \in \mathcal{C}$, which is non trivial. In what remain of this section, we shall present how to do such addition.

Let $\mathcal{C}$ be an ellitptic over the field $\mathbb{F}$ and let $P = (x_1, y_1), Q = (x_2, y_2) \in \mathcal{C}$. Then, the following cases hold:

- The points are opposite of one another, then $P + Q = P + \mathcal{O} = P$.
- The two points are distinct; then we consider the line that passes through them. That is, we compute

  $$x_3 = m^2 - x_1 - x_2 \qquad y_3 = m(x_1 - x_3) - y_1$$

  where $m = {}^{(y_2 - y_1)}/_{(x_2 - x_1)}$ is the slope.
- The two point coincide; then we consider the tangent line. That is, we compute

  $$m = \frac{3x_1^2 + a}{2y_1}$$

  and x_3, y_3 as before.

- 3 - Public-key cryptography.

Modern days cryptography is based on a set of protocols based on the concept of *public-key* exchange. We proceed as follow: the idea of public-key cryptography is defined first, then some protocols will be presented. For the latter we discuss both the algorithms and the mathematical hard problem these are based on.

- 3.1 - The public-key exchange protocol.

Proposed for the first time in [1], it was a breaktrhough in cryptography. The idea is that of crypting the message as some discrete value, by means of a one-way function; that is, a function that is easy to compute, but whose inverse is hard to compute.

The whole cryptosystem relies on the assumption that one-way functions do exists; through the years several have been proposed and are used in schemes we discuss in the following, yet these are not garanteed to be one-way[1].

- 3.2 - The RSA algorithm.

The RSA algorithm, from the name of its inventors: Rivest, Shamir and Adleman (see [2] for major details); is a public-key algorithm based on the hard problem of integers factorization.

Formally speaking, the Integers Factorization Problem (IFP) is defined as follow: given a positive integer n, find its prime factors; that is, find $p_1, p_2, \ldots, p_k$ such that $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, with $\alpha_i \geq 1$.

- 3.2.1 - The algorithm.

Let m be the message to transmit; to cypher it by the RSA protocol do as follow: begin by choosing two odd distinc prime numbers p, q randomly, such that their bitlength is approximately the same. Compute $n = pq$ and $\lambda = (p-1)(q-1)$. Let $\mathcal{B}$ choose an integer e such that $\text{GCD}(e, \lambda) = 1$; the pair (n, e) will be $\mathcal{B}$'s *public key*. Let d be the integer less then λ, such that $ed \equiv 1 \pmod{\lambda}$; this will be $\mathcal{B}$'s *private key*.

To encode the message $\mathcal{A}$ computes

$$c \equiv m^e \pmod{n}$$

and sends c to $\mathcal{B}$. Upon reciving the chypertext, $\mathcal{B}$ can easily decode m as

$$m \equiv c^d \pmod{n}. \tag{1}$$

[1] If one proves the existence of one-way functions, at the same time would solve the $\mathcal{P} = \mathcal{N}P$ problem.

To see why *Equation* (1) holds observe the following: since $ed \equiv 1 \pmod{\lambda}$, there exists k such that $ed = 1 + k\lambda$.

Now, we have that:

- If $\text{GCD}(m, p) = 1$ by Fermat's little theorem

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

  Hence, raising both sides by $k(q-1)$ and multipling by m yields

$$m^{1+k\lambda} \equiv m \pmod{p} \implies m^{ed} \equiv m \pmod{p}.$$

- If $\text{GCD}(m, p) = p$ the above still holds, as both sides will be congruent to 0.

Applying the same reasoning for q, since p and q are distinc, we conclude that

$$c^d \equiv m \pmod{n}.$$

Let us briefly overview why $\mathcal{E}$ cannot, at least no so easily, dechypher the message sent by $\mathcal{A}$. By the protocol both n, m are know to everyone, but the values of λ and d are not as these depend on p and$q$. Hence, the only choice left to $\mathcal{E}$ is to factor n; which we know is hard to do.

Example

Let $p = 37, q = 39$. We have $n = 1443$ and $\lambda = 1368$. Say $\mathcal{B}$ chooses $e = 263$ for is public key. At this point the pair $(n, e) = (1443, 263)$ is know to everybody. $\mathcal{A}$ converts is message into an integer $0 < m < n$, say $m = 1029$ and computes

$$c \equiv m^e \pmod{n} \implies 1320 \equiv 1029^{263} \pmod{1443}$$

and sends $c = 1320$ to $\mathcal{B}$. In the meanwhile, $\mathcal{B}$ computes d such that $eq \equiv 1 \pmod{\lambda}$, in our case $d = 671$. Hence, upon reciving $c, \mathcal{B}$ dechyphers it as

$$c^d \pmod{n} = 1320^{671} \pmod{1368} = 1029.$$

■

References.

[1] Whitfield Diffie and Martin E. Hellman. “New directions in cryptography”. In: *IEEE Trans. Inf. Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[2] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. In: *Commun. ACM* 21.2 (1978), pp. 120–126. DOI: 10.1145/359340.359342.

[3] 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

IFP Integers Factorization Problem. 6

LCM Least Common Multiple. 2