Notes on Data Encryption

Riccardo Lo Iacono

January 23, 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 $a \not| \, b$.

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 on 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 om 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 inerithed 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*

$$\mathrm{Ord}(H) \mid \mathrm{Ord}(G).$$

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 $\mathrm{Ord}(g) \mid \mathrm{Ord}(G)$.

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

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