mathematics

MDPI

Article

Some Notes on a Formal Algebraic Structure of Cryptology

Vicente Jara-Vera * and **Carmen Sánchez-Ávila**

Departamento de Matemática Aplicada a las Tecnologías de la Información y las Comunicaciones (Escuela Técnica Superior de Ingenieros de Telecomunicación), Universidad Politécnica de Madrid, Avenida Complutense 30, 28040 Madrid, Spain; carmen.sanchez.avila@upm.es

* Correspondence: vicente.jara@upm.es; Tel.: +34–686–615–535

Abstract: Cryptology, since its advent as an art, art of secret writing, has slowly evolved and changed, above all since the middle of the last century. It has gone on to obtain a more solid rank as an applied mathematical science. We want to propose some annotations in this regard in this paper. To do this, and after reviewing the broad spectrum of methods and systems throughout history, and from the traditional classification, we offer a reordering in a more compact and complete way by placing the cryptographic diversity from the algebraic binary relations. This foundation of cryptological operations from the principles of algebra is enriched by adding what we call pre-cryptological operations which we show as a necessary complement to the entire structure of cryptology. From this framework, we believe that it is improved the diversity of questions related to the meaning, the fundamentals, the statute itself, and the possibilities of cryptological science.

Keywords: algebra; cryptography; cryptology

MSC: 14G50; 94A60

Citation: Jara-Vera, V.; Sánchez-Ávila, C. Some Notes on a Formal Algebraic Structure of Cryptology. *Mathematics* **2021**, *9*, 2183. https://doi.org/10.3390/math9182183

Academic Editors: Angel Martín-del-Rey and Michael Voskoglou

Received: 9 July 2021
Accepted: 31 August 2021
Published: 7 September 2021

1. Introduction

Cryptology is a science that is usually explained based on its historical development. In the study of cryptography, its methods and systems, the various procedures and techniques, are explained: the Greek Skytalé, the substitution of Aeneas, the methods of the statesman and military general Gaius Iulius Caesar (100 BC–44 BC) and the emperor Gaius Iulius Caesar Octavianus Augustus (63 BC-14) [1], the polyalphabetic substitution of Johannes Heidenberg, OSB, known as Tritemius (1462–1516) [2], the Girolamo Cardano grille (1501–1576) [3] (pp. 95–97), other transposition ciphers (rows-columns, series, groups) [4] (pp. 102–111), and diversity of substitution methods, such as Thomas Jefferson (1743–1826) [5] (pp. 51–52), Charles Wheatstone (1802–1875) [5] (pp. 47–48), Edouard Fleissner (1825–1888) [5] (pp. 49–51), the matrix polygraphic encryption of Lester S. Hill (1891–1961) [3] (pp. 80–92) or the Playfair polygramic encryption of Charles Wheatstone himself [6] (pp. 100–102). Mention should also be made of the substitution by homophones [4] (pp. 44–50), a system to break the natural statistics of language that maintain the simplest transpositions and substitutions, as the polyalphabetic substitution systems also tried to do [4] (pp. 51–76). Throughout history, to improve the systems and hinder their cryptanalysis, some of these methods have been unified and applied together, as in the nomenclators, especially those used with profusion from the Renaissance to the 20th century [7] (pp. 107–119, 150–161); or several substitutions or transpositions, and even transpositions and substitutions jointly, as in ADFGVX encryption [3] (pp. 53–54).

The development of mechanical systems of wheels and grids since the Renaissance [8] (pp. 109–148), from the simplest, such as that of Leon Battista Alberti (1404–1472) [7] (pp. 125–130), and following among others, with the model of Gabriel de Collange (ca. 1521–1572) [5] (pp. 43–44), led to the construction of more complex concentric structures: the Edouard Fleissner or Charles Wheatstone variants [5] (pp. 47–51), along with the use of disc transposition, such as the Thomas Jefferson system [5] (pp. 51–52). From there, to the structure of discs chained sequentially, with the rotor machines [3] (pp. 110–126, 145–156) [9,10], from the first one of Edward Hugh Hebern (1869–1952), through those of Boris Hagelin (1892–1983) and the Enigma of Arthur Scherbius (1878–1929) of the second decade of the 20th century, or the Red-91-shiki injiki (Japan, 1930s), Purple-97-Shiki obun inji-iki (Japan, 1940s) and SIGABA-ECM Mark II (USA, 1940s), among others; or those manufactured with thermionic or vacuum valves, and ferrite cores such as ROMULUS (USA, 1950–1960) [11], to reach electronic devices with transistors and modern computer technology.

It was also the 20th century when the perfect secret system of Gilbert Sandford Vernam (1890–1960) appeared, specifically in 1917, although previously invented by Frank Miller (1842–1925) [12] (pp. 103–117). Then, in 1976 the DES encryption (Data Encryption Standard, FIPS PUB 46–3) was adopted, whose main developer was Horst Feistel (1915–1990) [6] (pp. 169–174), predecessor encryption of the current AES (Advanced Encryption Standard, FIPS PUB 197), standard symmetric encryption from the year 2002, by Joan Daemen (1965-) and Vincent Rijmen (1970-) [6] (pp. 175–178).

On the other hand, and at the same time, an unexpected event happened at the beginning of the last quarter of the 20th century, because in 1976 Whitfield Diffie (1944-) and Martin Hellman (1945-) in their paper “New Directions in Cryptography” [13] announced the discovery of asymmetric or public key cryptography, aspects also developed independently by Ralph Merkle (1952-) in “Secrecy, Authentication, and Public Key Systems” [14] in 1979. Until this moment all cryptography had always been symmetric, where the encryption and decryption key was the same. As of now, with this new type of cryptography, both keys are different although they are related, but one key cannot be obtained from the other through simple computational methods. It is the emergence of systems such as the RSA in 1978, by Ron Rivest (1947-), Adi Shamir (1952-) and Leonard Adleman (1945-) [15] (pp. 285–291); that of Taher Elgamal (1955-) in 1985 [15] (pp. 294–298), or that of Elliptic Curves in 1985–1987 by Victor S. Miller (1947-) and Neal Koblitz (1948-) [16]. However, asymmetric cryptography was secretly developed from 1944 and finally perfected in 1973 by James Henry Ellis (1924–1997), Clifford Cocks (1950-), and Malcolm Williamson (1950-), of the British Government Communications Headquarters (GCHQ), as recorded in the documents that were made public in 1997 [8] (pp. 272–291).

This itinerary, especially on asymmetric cryptography, capable of achieving authentication, is being extended towards the so-called post-quantum cryptography, secure against attacks by quantum machines. This new modality does not base its security on the problems of mathematical complexity as the aforementioned ones did (RSA, Elgamal, Elliptic Curves, and the like), for the use of the algorithm of Peter Shor (1959-), as NTRUEncrypt, by Jeffrey Hoffstein (1953-), Jill Pipher (1955-), Joseph H. Silverman (1955-), or the complete homomorphic encryption of Craig Gentry (1973-), and its subsequent variants, and possibly, the next cryptography to come [17–19].

However, this historical approach, being very enriching and instructive, needs to be complemented, we believe, with some foundations and a mathematical structure that supports it and shows cryptology as a fully-fledged branch within algebra. Something which, on the other hand, has been done and achieved in recent decades.

This work is from the cryptological field, but as will be seen in the historical sections, sometimes we will also find steganographic uses along with cryptographic ones. From the work of Shannon [20], we consider the concept of secrecy in both its steganographic and cryptographic sense (mainly in the latter for the object of the work) since we mention both in this study. Thus, we speak of secret insofar as concealment system, in which the existence of the message is concealed from the enemy; and also, and more commonly, in the sense that the message is concealed by cipher, but its existence is known, not hidden from the enemy or attacker.

We indicate that the principles of Kerckhoffs [21] do not alter the classification offered here, despite having considered both cryptography and steganography, although they are always desirable to be fulfilled in any secret system, if possible.

It is worth mentioning that from Shannon's theory we can say that there is perfect secrecy if the ciphertext and plaintext are statistically independent. Here, a passive adversary can learn nothing about the plaintext from the ciphertext, except possibly its length, even with infinite computational resources. To achieve this, the key is at least as long as the message. However, with keys shorter than the message, which is usual, it is expected that at least the so-called semantic security is achieved, expressed as a polynomially bounded version of perfect secrecy, whereby a passive adversary with polynomially bounded computational resources can learn nothing about the plaintext from the ciphertext [15] (pp. 42–43, 307).

2. Our Purpose: The Algebraic Foundation of Cryptology

Cryptology began as an art rather than a science, and it has been especially so since the middle of the 20th century when it reached a scientific-technical status, located in the broad field of applied mathematical science.

This maturity was reached with the work of Claude E. Shannon (1916–2001) and his paper "Communication Theory of Secrecy Systems" in 1949 [20], preceded the previous year by "A Mathematical Theory of Communication" [22]. Without trying to be exhaustive in the list of authors to mention, as this is not our goal, we would like to highlight the efforts in this direction of Charles Babbage (1791–1871) [7] (pp. 204–207), Maurits de Vries (1876–1943) [7] (p. 737), Gaëtan H. Léon de Viaris (1847–1901) [7] (pp. 240–242), or the aforementioned Lester S. Hill [7] (p. 739), and around the same years as Shannon's publication [20,22], the works of Abraham Adrian Albert (1905–1972) [7] (pp. 410, 677, 737, 739) [23] and William F. Friedman (1891–1969) [24–27]. As Abraham A. Albert stated in a regional meeting of the American Mathematical Society in 1941, *it would not be an exaggeration to state that abstract cryptography is identical to abstract mathematics* [23].

These foundations are what the later cryptological developments are based on, and which we find in the different manuals and main bibliographic works in this discipline [3,7,15,24–31]. In these works, we find a very successful attempt at mathematization and formalization, with multiple algebraic components and structuring that speaks of functions, bijections, injective and surjective maps, or even permutations, as well as compositions of functions, and next to it, endomorphisms, which also deals with the encoding of several elements at the same time, as well as matrix expressions for various systems. However, we believe that we need a greater systematization and precision that fully and comprehensively exposes all cryptographic systems and methods. With that some new elements should be offered that help us to better understand the entire field of cryptographic fundamentals.

We hope to shed light on this area with this paper. For this, we will begin by systematically reviewing, as a first approximation, the various cryptographic systems used throughout history, which in the next section will help us to show a complete and new organization of them, this time, already compact and complete.

Finally, based on the new proposal, we will gather some clarifications and explanations regarding the perfect cipher and the ideal cipher, as well as the distinction between block and stream ciphers, on the one hand, and the division between symmetric and asymmetric encryption on the other.

3. Cryptographic Methods and Systems throughout History

We will compile the various forms of encryption that have emerged throughout history in a synthetic way, giving a first structuring that will serve as an organized classification and that we will subsequently modify to a more standardized and complete systematization.

The main classification of cryptography, which is the usual categorization, is that which divides it into methods of transposition and substitution.

3.1. Cryptographic Methods

3.1.1. Transposition

Throughout history, the following, among others, have been applied. These are the main ones, and can give us a broad idea of the diversity of use of this method.

- *Inverse or reversed.* The text is written starting with the last letter until it reaches the first, letter by letter. Sometimes the syllables, or the words, are reversed [5] (p. 23).
- *Boustrophedon.* A simple linguistic method in which the direction of writing sometimes changes alternately (left–right–left–right–. . .). In others, it is even done with specular writing in alternate sentences [32] (pp. 140–141).
- *Temurah.* This is a method of the Kabbalah or Jewish mysticism consisting of the rearrangements of the letters in each of the words in the text, that is, word-by-word transpositions [7] (p. 92).
- *Geometric.* These make a reading of the text arranged in geometric forms, following horizontal–vertical two-dimensional placements, according to columns, in zigzag, using two-dimensional tables, according to gnomons or other geometric forms, systems among which we have the Lacedaemonian Skytalé [5] (pp. 22–28).
- *Disjoint partitions or series.* In this case, the text is divided into disjoint sets; for example, letters of order as prime number, letters of order as non-prime even number, and finally, the odd non-prime letters—and are rearranged by placing the elements of the plaintext according to those sequences [4] (p. 104).
- *Grille.* This method was invented by the physicist and mathematician Girolamo Cardano, consisting of a system of the orderly placement of letters (or even syllables or words) according to a lattice, which was already discerned by Jacobus Silvestri (ca. XV–XVI) and Ibn al-Durayhim (1312–1361), and was perfected in the 18th–19th century. In short, it is a distribution of the grams or elements in a regular n-polygonal figure of elements after a placement in $\mathbb{N}^2$ inside, and then, a symmetrical vector scan is performed n times until the polygon and all its elements are finished [3] (pp. 95–97) [7] (pp. 144–145, 180, 308–309). Sometimes to facilitate the construction of the grid or lattice, a certain agreed method was followed with the use of a keyword previously replaced by numerals that would help to place all the letters, sequentially arranged, of the message, such as Colonel Roche's method [33] (pp. 117–118, 123–125).
- *Groups of permutations.* The message is divided into small blocks, n-grams, of equal length, or not. Each of these blocks is subjected to the same permutation of its elements throughout the text (sometimes the permutation could be changed throughout the message). An example is Cardinal Richelieu's encryption (1585–1642) [5] (pp. 24–25).
- *Anagram.* It is the reordering of letters in a phrase or word, sometimes without a clear meaning, to obtain a new expression of similar semantics or not, such as the examples we have of the correspondence of Galileo Galilei (1564–1642), who in a letter dated 1610 sent the following message to Johannes Kepler (1571–1630): "SMAISMRMILMEPOETALEVMIBVNENVGTTAVRIAS", which Kepler managed to decipher as "salve, vmbistinevm geminatvm martia proles" ("hail, fiery twins, progeny of Mars"), making Kepler think that Galileo had discovered two satellites around Mars. However, the initial solution generated by Galileo was "altissimvm planetam tergeminvm observavi" ("I observed that the highest planet was triple"), referring to Saturn, which he seemed to visualize with two satellites, unable to see that it was its rings. In the most complicated case of the anagram, only the cast of times of each of the letters appears, with no more information [3] (pp. 102–105).

3.1.2. Substitution

The greatest diversity of systems has occurred in the substitution over time, offering a very wide range of ciphers, which we can even subdivide into large families.

Monoalphabetic

In these systems, the same element of the message or plaintext is replaced by another element, but always the same element, in the encrypted set.

- Monogramic. It is the substitution of one gram, 1-g, or origin element for another (or others, n-grams) different from the destination set and always for the same. The most common throughout history are as follows.

  - *Rebus, acrophony, logogram, ideogram, pictogram.* They are iconic and hieroglyphic forms of diverse substitutions. Thus, the rebus is the correspondence of ideograms or pictograms in which the first syllable or letter gives its name [32] (pp. 487–503); by acrophony, the graphemes of a language acquire the name of an everyday object of similar appearance and denomination such that its first letter is just that referred to in the alphabet, an aspect that we find in the emergence of the graphemes we use in the West [7] (pp. 71–73); in the logogram, a single symbol has the full meaning of a concept or object [7] (pp. 75–76); the ideogram collects unconventional signs, with a relationship between the sign and the referent, and linguistically conditioned [34] (pp. 30–31); the pictogram is the iconic figuration of the object or concept it represents [32] (pp. 487–503).
  - *Reverted or Atbash.* Substitution of Semitic origin that changes each letter of the Hebrew alphabet, which we will call $\aleph$, in the corresponding one according to the expression $x' = Card(\aleph) - x$, in which $Card(\aleph) = 22$, in the manner of an inverse or specular image with the separation axis on half of the alphabet [7] (pp. 76–78).
  - *Albam.* This system applies a partition into two groups of $Card(\aleph)/2$ elements on the Hebrew alphabet and replaces each letter according to the expression $x' = x + Card(\aleph)/2 \; mod \; Card(\aleph)$ [7] (pp. 78–79).
  - *Caesar, Augustus, and other affine forms.* Here there is a shift of the letter of the plaintext by the substitution letter 3 positions, such as the Gaius Iulius Caesar system, or only 1 shift, as the historically later system of Gaius Iulius Caesar Octavianus Augustus. Thus, the substitutions follow the forms $x' = x + 3 \; mod \; Card(A)$, and $x' = x + 1 \; mod \; Card(A)$, or generally, in their affine form, as $x' = ax + b \; mod \; n$, A being the set of alphabetic elements, and a, b and n integers [4] (pp. 29–43).
  - *Letter (vowel or consonant) preceding, next to or adjacent $\pm i$ positions.* These are substitutions that we find in some medieval manuscripts, in which certain letters, such as vowels, or consonants (sometimes not all), could be replaced by the next letter in the alphabet, or the preceding one, or by the one at certain distance from it in an ordered alphabet. It is, therefore, a partial affine encryption, applied to only some elements of the message [35] (p. 4).
  - *With key-word or key-phrase, pangram or random.* All of these are methods of complicating the system of replacing the original alphabetic elements with the encrypted ones, making the correspondences, the binary relations, between origin and destination elements as random as possible [36] (pp. 76–79, 98).
  - *Polybios.* Alphabetical square system 5×5 of substitution of monograms in bigrams, devised by this Greek historian (ca. 200 BC–118 BC) [1] (pp. 147–148).
  - *By gender, type, or semantic groups on each letter.* Generally, short messages undergo the total or partial substitution of letters by a series of elements of a semantic set, such as the names of birds, planets, etc., sometimes pictorially, as we already have in Ibn al-Durayhim's work. As we can see, it is a substitution of 1-g (letter) to n-grams (words of different lengths) [7] (pp. 94–98).
  - *In general, the substitution of 1-g to {1, 2, 3, . . . }-grams.* For example, the one used by the Soviet NKVD, in which each letter or 1-g symbol had the option of 1-g or 2-g [7] (pp. 641, 650).

- Bigramic (2-g to 2-g), and in general, n-gramic to n-gramic. Giambattista della Porta (1535–1615) was the inventor of the 2-g monoalphabetic substitution system to 2-g [2] (pp. 291–292), a scheme from which the generalization of n-grams to n-grams is possible, as we find in various nomenclators or the Playfair system [6] (pp. 100–102) or the matrix system of Lester S. Hill [3] (pp. 80–92).
- {1, 2, 3, . . . }-gramic to {1, 2, 3, . . . }-gramic. It is the case of maximum generalization, in which the set of departure can have any length of grams and the destination set can also have different lengths, always replacing the same origin block or n-gram with the same n-gram destination.

As an example, we can highlight the codebooks and dictionaries, which we will see in a later section for their particular historical importance [7] (pp. XVI, XVII, 177).
Another fascinating example is the use of the translation of a message from one language to another, which apart from the homophonic and polyphonic diversity present, due to the freedom existing in the translations, we can place here, and that, in the case of it being a very little known language, the language for encryption, can be very difficult cryptanalysis in the sending of messages, especially audio messages, as happened with the language of the Navajo Indians in World War II by the U.S.A codetalkers [7] (p. 550).

Polialphabetic

In this system, the same element of the message is replaced by different elements in the encryption set, depending on the key that is being assigned.

- Monogramic. Each origin 1-g is replaced by the destination element of the alphabet that corresponds in each case.
  Leon Battista Alberti in the 15th century created the first known polyalphabetic substitution cipher [7] (pp. 125–130). He used a mechanical system with two encryption disks with the same center. After the encryption of several words, the alphabet was changed, having previously agreed on the opposite letters of both discs at the beginning, and indicating the next alphabet change by inserting the letter of the new correspondence into the encrypted message, in the text, marking the change with a capital letter, an aspect that can be masked in a second information, as a secret key, therefore through the pseudo-randomness of these changes it becomes safer than the historically later polyalphabetic modalities of Tritemius, Belasso, della Porta or Vigenère.
  In this manner, Johannes Heidenberg, O.S.B., also known as Tritemius, would create the so-called "tabula recta" or "flat board", with 24 alphabets, sequentially ciphering and changing the alphabet (that is, taking the next letter of the key) after each letter of the plaintext [7] (pp. 130–137). Giovan Battista Belasso (1505-ca. 1565) eliminated the rigidity of the sequentiality of the alphabet from the "tabula recta", thus providing the lateral key, the reciprocal key, the agreed verse key, the word key, meaningful or not, the irregular or messy key, the syllabic and the rotational key [7] (p. 137). On the other hand, Blaise de Vigenère (1523–1596), as a compiler of previous works and without improving the previous forms, used words, phrases, verses, or a progressive use of a key [7] (pp. 145–150), aspects that Giambattista della Porta also spread [7] (pp. 137–143).
  Its generalization would be the case of the polyalphabetic substitution of 1-g to {1, 2, 3, . . . }-grams.
  Let's see some of its variants:
  - *Progressive or sequential by letters.* When enciphering each letter of the original text, the following alphabet is used consecutively according to the sequence of the letters of the alphabet, a method we have seen with the "tabula recta" of Tritemius [7] (pp. 130–137).
  - *Sequential by blocks.* The alphabet is not changed except when encrypting several letters, maybe one or several words, etc. Examples of this system are the original of Alberti [7] (pp. 125–130), or the Phillips military cipher [37] (pp. 185–191), that every five letters changes the replacement alphabet, or that of Wheatstone, that by means of a mechanical system of two discs and two needles, when turning a complete revolution, the longest needle that marks the encrypted letter, the smaller needle marks the new alphabet to be taken, following a period system in the manner of clockwise in its displacement [5] (pp. 47–48).
  - *Key-word or key-phrase.* A word or literal sequence, a phrase, which is repeated, serves as a key to encrypt all the plaintext. They are the majority of options that we have seen with Belasso, Vigenère, or della Porta [7] (pp. 137–150).

  - *Autokey.* In this case, the key is originated from the material used, either from the plaintext or from the encryption text. Cardano himself intuited the autoclave form, albeit with errors, by placing the same clear text as the key, beginning with each word to be encrypted. Belasso managed to improve it by encrypting the first word with a Tritemius-type polyalphabetic system and subsequent words by taking the previous word in its first letter as the beginning of the sequentiality of the polyalphabets. Vigenère perfected it using an agreed prior letter, which allowed subsequent stream decryption from the subsequent plaintext letter as the next letter of the key, or even using the encrypted text [7] (pp. 143–147).
  - *Random.* With Alberti himself, we have found randomness in his choice of keys, although after encrypting several words. In this case, it is intended to do so for each letter. In the key-interrupted mode, a sufficiently long keyword was taken, which was cut in certain ways several times and subsequently joined together again, allowing a certain diversity in the encrypted result, although it ended up looking for a key as long as the plaintext, the so-called running-key [37] (p. 143), although the best option was for the encryption key to be completely random, aspects suggested by della Porta or Fredrik Gripenstierna (1728–1804) [3] (pp. 131–132), offering maximum security. This is the case of the Vernam encryption, the perfect substitution cipher [3] (pp. 141–171).

- Bigramic (2-g to 2-g), and in general, n-gramic to n-gramic. A different substitution of a 2-g block to a 2-g block is obtained utilizing a key, such as the one found in the Slidefair encryption [37] (p. 199).

  It is clear that this system can be generalized in a polyalphabetic of n-grams to n-grams.
- {1, 2, 3, . . . }-gramic to {1, 2, 3, . . . }-gramic. It would be the case of maximum generalization, in which the initial set can have any length of grams and the elements of the destination set can likewise have different lengths, with polyalphabetism depending on the key used.

Homophonic

In this type of encryption of an element of the plain message, an element of the origin set can be replaced by more than one element of the encryption destination set. It can be applied to some elements or all of them, and with two or more destination elements for each of the substitutions, even with the same or varied types of elements for each homophony [3] (pp. 44–46) [5] (pp. 68–71, 94–106).

Because of its importance in history, it is worth noting that from 1401 we note the first homophony case in the Mediterranean area of Christian influence, and in a more systematic way than ever before, clearly seeking the security of encryption, in correspondence between the court of Mantua, in Lombardia, and Simeone da Crema (ca. XIV–XV), with four possible substitutions for the vowels {a, e, o, u} [7] (pp. 107–108).

However, before that, we find it used by Duke Rudolfs IV of Austria (1339–1365) in an alphabet of pseudo-Chaldean or symbolic characters, a monoalphabetic substitution cipher with homophony duplicated for five letters and triplicate for one letter [35] (pp. 11–13). However, its first appearance seems to be in an anonymous work of the Abbasid caliphate in the 10th century, applied to the two most common letters, with substitution of three possible elements [36] (pp. 20–23, 62–64); reappearing in the 13th century in the first cryptanalysis manual, the work of Alif al-Mutargim (1187–1268), applied to the blank spaces between words [38] (p. 19).

Polyphonic

This has hardly ever been used, due to the ambiguity in decryption, since the same letter in the destination may correspond to more than one different letter possible in the origin set.

We can cite the case of the Bavarian abbey manuscript by Ellinger von Tegernsee (ca. 978–1056), MS. Cheltenham 816, of the 11th century, where in addition to simple substitutions it uses homophony and polyphony, transforming the vowels "a" and "e" into the same letter, the letter "H" [35] (p. 5); a method that is also rarely used, and for no more than two or three elements of the cryptographer Matteo Argenti (1561–ca. 1610) [7] (pp. 112–114).

Codebooks and Dictionaries

Systems that we have found since the end of the Middle Ages and that would become increasingly wide and complex, up to the World Wars of the 20th century. They are systems applied to letters, syllables, words, expressions, or phrases, that is, $\{1, 2, 3, \ldots\}$-grams of any length, almost always to specific n-gram encryption (which is usually numerical), of a certain length. In short, and in general, it is a particular case of monoalphabetic substitution of $\{1, 2, 3, \ldots\}$-grams over $\{1, 2, 3, \ldots\}$-grams.

They began to become longer and longer lists of words and expressions, the so-called codebooks, and with the passage of time, and due to their becoming increasingly large and unmanageable, especially in the decryption process, also forced to order these values in the so-called code dictionaries [7] (pp. 177–186, 216–223, 314–324).

Nomenclator

This is the union of several already considered systems. It is a particular case of monoalphabetic, or even polyalphabetic, substitution in any of its forms, using letters, numbers, or any possible symbol, perhaps with homophony, and with the use of codes or dictionaries. It has been one of the most used systems from the Renaissance up to the middle of the 20th century [7] (pp. XVII, 106–124, 160–192).

3.1.3. Arithmetic-Algebraic Operations

Having seen transposition and substitution, the two great traditional methods throughout history, with their various subdivisions, modalities, and variations, sometimes, more or less simple mathematical operations were also used. The realization of operations on the elements supposes a previous substitution of the graphemic literals by numbers, on which arithmetical operations (the basic operations of addition and product and their inverse) are commonly applied, or more generally, the operation of the algebraic group. It would be, therefore, more precisely, a case of internal composition between two types of substitution, the first to numerals and the next to the new number resulting from the operation.

Let us look at the systems most commonly used over time.

- *Atbah.* This is a substitution of Semitic origin that starts from the numerical-alephatic equality to give numerical values to the words (from the values of their letters), and from these values to look for words that give similar sums, although with several possibilities: thus, sometimes the figures and values of the units, tens and hundreds, are obtained from the Hebrew alphabet, while on other occasions it considers the base-22 (number of letters of the Hebrew alphabet), so that two letters are matched and can be substituted between them if its sum gives that number. Alternatively one letter can be substituted for two letters that give a sum similar to the previous one. Examples of this type are not found in such recent dates as in the conformation of the Hebrew biblical text, but in the Babylonian Talmud, from the 5th century of our era, thus identifying both senses, in response to the search by the mystics of the Judaism of solutions to divine and prophetic questions hidden in the sacred text [7] (pp. 79, 91–92). We find a similar system in the Muslim world in the Arabic "hisab al-gummal" of 28 letters, with the assignment $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000\}$ [39,40]. Or the case not yet in Hebrew, but in Greek, because we are on this occasion mentioning a Christian book written in Greek, in which we find the number 666 (in almost all papyri and codices) or 616 (according to the P.Oxy. LVI 4499 papyrus), primarily in the text of Revelations, in the

Christian New Testament, in chapters and verses 13, 17–18 and 15, 2, referring either to emperor Nero (37–68) or emperor Domitianus (51–96) [41] (p. 13).

- *Duplicate, triple, . . . , or divide and other forms of the product and its inverse operation.* This is a method based on the conversion of literal n-grams to numerical n-grams to obtain other figures later and leave them as a mere numeral sequence, or hidden in mercantile texts (thus using stereographic aspects), as we find, using the substitution "hisab al-gummal", in the work of Ibrahim ibn Dunaynir (1187–1229) [42] (pp. 22–25, 68–70).
- *Subdivide the numerical values of each letter or gram into sum components (two, three, or more) and other forms of additive operation.* Possible forms within the Muslim "hisab al-gummal" [39,40] and which we also found in the Armenian people in the 16th century, being substitutions with homophony [7] (pp. 85–86).
- *Any other integer or modular arithmetic operation on the numbers after the previous replacement of the message grams.* Among them, we can cite the related ciphers, of expression $Enc(m) = am + b \; mod \; n = c$, already considered, generalizations of the Caesar and Augustus substitutions; even the variant that we find with the encryption of Léopold François Auvray (1819–1876), where after replacing the letters with numbers, both in the clear text and in the key, both are added, which is still a polyalphabetic encryption, although numerical [5] (pp. 64–65); or the most complex contemporary forms and that we find in the asymmetric RSA, Elgamal or Elliptic Curve ciphers, among others [43] (pp. 354–384), which we will mention later.

3.2. Other Methods

However, despite the usual assumption that we would have already exhausted the spectrum of cryptological options having reviewed the transposition and substitution methods, as well as arithmetic-algebraic operations, we must indicate that other methods that are not properly cryptological modes have been used throughout the history of cryptology. We consider the ones which should be collated here, for reasons of completeness, which we will clarify later in their foundation, and are the deletions and insertions of elements on the original plaintext of the message.

Elimination

We mention the following as historical examples of elimination:

- *Elimination of some vowels and/or consonants in the clear text of the message.* A system found in some European medieval codices, with the elimination of some vowels and consonants [35] (p. 4), referred to as the Benedictine method by some authors [33] (p. 138).
- *Pruned text.* This verbal ludic-linguistic type consists of taking smaller fragments of words in a text, also becoming known from early dates [32] (pp. 316–329). Thus, we find it in some Alexandrian magic papyrus of the 3rd and 4th centuries of our era, with magic words of spells and enchantments such as "Abrakadabra", "Abrakanarba", "Ablanatanalba" or "Abraxas", generating new words with or without meaning by eliminating one literal after another, minor and powerful forms of the same original enchantment [44] (pp. 17, 31, 34, 68, 76, 89, 127, 248, 280, 320).
- *Acronym.* This is the composition of a new word from a set of words taking the first of their letters or their first syllables. It is a linguistic-verbal figure well-known since ancient times in examples such as "SPQR", "Senatus Populusque Romanus" ("the Senate and the Roman people"), or "INRI", "Iesvs Nazarenvs Rex Ivdaeorvm" ("Jesus Nazarene, King of the Jews") [32] (pp. 249–254).
- *In general, the elimination of any amount of {1, 2, 3, . . . }-grams.* Here, we would have the possibility of removing any number of letters or symbols under any rule, in short, {1, 2, 3, . . . }-grams.

Insertion

We can cite the following as historical examples of insertion:

- *Insertion of some letters or syllables in certain places of the clear text of the message.* It is the introduction of letters, sometimes syllables, in certain places of the message text, sometimes in odd or even places, etc., with the consequent withdrawal of them for the deciphered reading of these insertions; or the insertion into the first letter of the first word, then in the second letter of the second word, and so on; and similar forms. Some examples of this system can be found in the work "Steganographia" by the cryptologist Tritemius [2,45] (pp. 283–287).
- *Insertion of words and phrases in the clear text of the message.* Examples of this method can also be found in the work of Tritemius, in which words and even complete phrases are introduced into the Latin texts of the original message [2] (pp. 283–287).
- *Subliminal channel.* This system can be seen as a method of inserting foreign words into the text, generally applied to literal grams, since its purpose is to hide the meaning, and therefore we can also see it as a steganographic method, placing the main text message within another larger text [33] (pp. 228–232).

  We can cite as an early example the comment by the Muslim cryptologist Ibrahim ibn Dunaynir, or the systems of the generation of literary texts, in verse or prose, used in later centuries, from which only certain lines had to be read, leaving the rest, to understand the real meaning [42] (pp. 13–14, 44–49, 136–153).
- *Notaricon and acrostic.* Notaricon is a cabalistic method consisting of taking the first letter of the respective words of an intelligible text, or sometimes without clear and precise meaning, to obtain a new word, key to the meaning of the original text [7] (p. 92).

  For its part, and generalizing to the aforementioned, acrostic is the composition that arises by reading the first, or certain predetermined letter, sometimes two or three initial letters or the first and last, of a word or phrase, of a set of words taken horizontally, vertically, diagonally or in another specific geometric shape, obtaining another word or text. The options as we can see are numerous, some with their names: thus, if it consists of taking the first letter it is called acrostic, just like that; but if we select the central letter it is called mesostic; or if it is the final one, we would talk about teleostic; or if it consists of making a diagonal reading from the upper left we would have the catadiagonostics; and if it is from the bottom left it would be an anadiagnostic; and with the labyrinthine form we would have a kind of technopaegnion, almost a calligram, in which the letters form an image according to the meaning of the text, although without reaching it, staying in a magic square shape or close to a crossword puzzle [32] (pp. 188–248).

  These types of examples have been known since classic times, this being the way the author of the Castilian work (from Spain) "La Celestina", Fernando de Rojas (ca. 1470–1541) was hidden, or King Alfonso X of Spain (1221–1284) in "Las Siete Partidas".
- *Null insertion.* This consists of inserting null or invalid values, that is, without semantic meaning for the original message, into the text, once it has been encrypted, confusing the cryptanalytic process. We found it cited early in the 10th century by an anonymous author in the Muslim lands of the Abbasid caliphate [36] (pp. 9, 62–64, 77–87, 102–104, 116), although from the Renaissance it was widely used until well into the 20th century [7] (pp. 106–124, 333–337, 763).
- *In general, the insertion of any amount of {1, 2, 3, . . . }-grams.* This method can be generalized under any rule such as the introduction of any number of grams or symbols of any type or length into the encrypted text or the message text.

  A historical method that we have to mention here is that of the nullifiers, that appeared in the year 1483, which we find in the Milanese ciphers: two symbols that converted the sign in between without semantic utility, an aspect that will be developed in the following nomenclators, sometimes using a single nullifier and applying it to the preceding sign, the next one, or for all the signs until the end of the line; a system that would become habitual in the following two centuries in the chancelleries of the European continent [7] (p. 111).

3.3. Composition of Methods

A detailed analysis of the different systems used throughout the broad history of cryptology also allows us to find some more that cannot be framed or placed in the previous ones, although they are their compositions: compositions of transpositions, substitutions, mathematical operations, eliminations, insertions, and even a method that is outside of cryptology, which would be steganography, although it has been part of the history of the concealment of messages.

In this way, by the composition, we consider the successive application in any form, order, and number of times, of the methods mentioned (including steganography) to generate new systems; something that we had already found in Ismail al-Kindi (801–873) when it refers to superencipherment, which is nothing more than the composition of two or more simple methods [46] (pp. 32, 132, 142, 144).

We collate the most common below:

- *Successive transpositions.* The composition of transpositions is a transposition, although looking for greater complexity and randomness in the encrypted text.
  Among the best-known are the nihilistic cipher, based on transposing the columns first and then the rows following the alphabetical order of two keywords, on a text arranged in a quadrangular structure [37] (pp. 17–19). Or the encryption of Émile-Arthur Soudart (ca. XIX-XX), which performs two successive transpositions utilizing a system of wheels placed on an axis [5] (pp. 28–29).
- *Successive substitutions.* The composition of substitution ciphers is still a type of substitution, although more complex, in principle.
  These are methods that we have already found throughout history, for example, in the numeral "tabula recta" [33] (pp. 152–153), using the Tritemius "tabula recta" system and the subsequent substitution by numbers, or in the aforementioned Auvray method [33] (pp. 157–158), literal substitution to numeral with subsequent polyalphabetic replacement. Others are very similar to these, such as the Gronsfeld system [37] (pp. 117–118) or the nihilistic substitution cipher [7] (pp. 620–621), both a literal-numeral substitution followed by a Vigenère polyalphabetic substitution.
  Among all of them are also the rotor machines, such as the Enigma of Scherbius, or those of Hagelin or Hebern, among others. These rotor machines, so popular in World War II, and subsequent years, despite their complexity, are still progressive-key polyalphabetic substitutions with a mixed alphabet and in general with a period based on the number of alphabetic letters [7] (pp. 408–434) [8] (pp. 131–193).
  Furthermore, the encryption of the naval Enigma variant should be noted here, which applied a new replacement of 2-g to 2-g to the rotor machine's encryption [3] (pp. 61–63, 122).
- *Substitutions and transpositions (and vice versa).* These systems make a substitution on an already transposed text, or a transposition to an encryption obtained by substitution, or combinations of these two methods, as many times as desired.
  In the work of Ibrahim ibn Dunaynir, we find the mention of systems that after a stage of encryption as a monoalphabetic monographic substitution was subsequently permuted or transposed [42] (pp. 7–15, 28–36, 58, 76–82, 100–114, 126–140). Other famous systems are the Thomas Jefferson cylinder [7] (pp. 192–195) or the Étienne Bazeries system (1846–1931) [7] (pp. 247–250), where the transposition of the discs is used to generate the disordered alphabets of the subsequent polyalphabetic substitution.
  Another example is the encryption of André Lange (ca. XIX-XX), which performs a vertical transposition in two lines of text and then replaces 2-g to 2-g [5] (p. 66).

Another system, with n-grams, is the case of a cipher used in the American Civil War, in which we find the transposition of words, having also replaced some of them, such as certain names, objects, places, or times with other words, due to their strategic importance [7] (pp. 225–226).

As examples used in World War I, we highlight the use of substitution and transposition composition in the famous German cipher of World War I, the ADFGVX system [12] (pp. 188–206); and also the combined Vigenère encryption with transposition [7] (p. 304). Another example very similar to the latter is the Nicodemus encryption, of the American Cryptogram Association, which after a Vigenère substitution performs a transposition according to a numbering scheme obtained from the key [7] (p. 763).

There is also, of course, the use of various compositions, such as the cipher of Félix Marie Delastelle (1840–1902), the so-called bifid system (although he also offered a trifid system), which is definitely a composition of three systems: It begins with a substitution of the letters of the alphabet (1-g) to a pair (2-g) of coordinates (x_i,y_i) according to a 5 × 5 table disordered by a word key. Subsequently, a transposition is applied by reading the odd elements (the x_i coordinates) followed by the even ones (y_i coordinates) and then composing it with a new substitution (2-g to 1-g) in the previous table [7] (pp. 242–244) [37] (p. 210).

- *Substitutions and homophony.* We have already found this composition of systems in the nomenclators [7] (pp. XVII, 106–124, 160–192), the examples becoming numerous over time.

  We can complete more this composition of methods here, as well as citing the official system of the Spanish Ministry of War of the late 19th century, composition of polyalphabetic substitution and homophony [33] (pp. 189–208). Or that created by the Spanish lieutenant Joaquín García Carmona (1857–1912), which is nothing but a substitution of the syllabary of a language, that is, of 1-g, 2-g, 3-g and 4-g (options of the syllables of the Spanish language), and for some more common with homophony, and substitution by numerals [33] (pp. 235–244).

  Another case, also of this type of composition, is to take a book agreed on by both the sender and the receiver, replacing each letter (or each word) of the message with numerals that give the location, that is, page-line-word-letter, having as expected homophonic cases, as was the system used by Hindu independentists during World War I [7] (pp. 371–372).

  Likewise, encryption by alphabetical groups, which starts from a Polybios with numerals, thus converting the literal 1-g to numerical 2-g, to later take for each numerical number (1-g) one word with that number of letters, that is, {1, 2, 3, . . . }-grams, therefore, with homophony [5] (pp. 58–59).
- *Successive codebooks.* This method consists of encrypting with a codebook to apply the result as an entry in a different codebook. As an example, the one found in World War I by the United States, where, after obtaining the 4-g from the first codebook of phrase and word codes, it was re-encrypted by taking smaller blocks of 2-g, in another codebook of digrams to words or phrases [7] (pp. 329–330).
- *Codebook and transposition.* An example that we find in a system by F. J. Sittler (ca. XIX-XX), which used the transposition of the numeral obtained in the codebook, which, in its four figures, gave the page and the line of the word origin of the message in clear text, which is still a substitution (by codebook) and subsequent transposition [7] (pp. 251–252).
- *Codebook, transposition, and codebook.* As an example of this composition, we know that it was used by some groups of smugglers in the mid-20th century, who hid their heroin traffic messages using codebook substitutions to subsequently make a change of digit position and then choose a new code word [7] (p. 817).

- *Codebook or nomenclator, and substitution.* In these cases, monoalphabetic or polyalphabetic encryption was performed as a result of previously encrypting with codebooks or even with nomenclators, as was used in the 19th and 20th centuries by various Western war embassies [7] (p. 251).
  On other occasions, a first substitution was made from the words of the message to a 4-number code, and then, after a new partition of blocks or n-grams, the numeral pairs were replaced by 2-g, a system used by the French army in World War I [7] (p. 312).
- *Codebook and homophony.* This system has already appeared in the nomenclators, although now more systematically with longer and extended codebooks. An example is found in the Cypher SA cipher of J. C. F. Davidson (ca. XIX-XX), from 1918, where, after replacing the words or set of words in the codebook, it allowed homophony for very common words [7] (pp. 278–282).
- *Multiple biliteral: substitution and steganography.* This is a system that we owe to Francis Bacon (1561–1626), substitution and steganography cipher composition [7] (pp. 882–884), the latter consisting of a binary distinction as to the type of typography, in short, a typographical, and therefore symbolic, substitution in a neutral text that hides the true message; and that it is possible to extend with the triliteral by Johannes Balthasar Friderici (1639-ca. 1704), considering three types of typography, or quantity of syllables of the words of the steganographic text [37] (p. 7).
- *Agreed language: {1, 2, 3, . . . }-grams to {1, 2, 3, . . . }-grams monoalphabetic substitution and steganography.* It is a particular case of monoalphabetic substitution of any quantity of grams over any other quantity of grams, with a semantic sense (trade, fauna, flora, etc.) in the encrypted text, thus maintaining a steganographic aspect. We already have examples from the Middle Ages, sometimes offering homophonic substitutions, or insertions of words in agreed places (at the end or beginning of the sentence, odd or even lines, etc.) [33] (pp. 222–228).
- *Substitution and mathematical operations.* An example of this type is the substitution of the letters of the message to numerical {1, 2}-grams, to later take the numerical key from a previously agreed base book, with a multitude of quantities listed in it, proceeding to the sum base-10 of the 1-g, just as the forces of the U.S.S.R. did during World War II [7] (pp. 650–654).
- *Substitution, transposition, and mathematical operations.* An example found in the Herrera system, a 19th-century Spanish soldier, consisting of replacing each letter of the alphabet with the first prime numbers, to finally give the product of the result, pending at the time of deciphering, order and arrange the primes now permuted or transposed [33] (pp. 221–222).
- *Subliminal channel: insertion and steganography.* We have already mentioned this system, this being its most proper place as it is a composition of systems. It is the insertion of foreign or strange words into the text of the message. This is found in Ibrahim ibn Dunaynir, who comments in his work on the insertion of the clear text, the message, within another larger text, as a subliminal channel [42] (pp. 13–14, 44–49, 136–153).
  Furthermore, the diversity of acrostics, with one letter or more, not always the first, sometimes taking a certain order, or with the use of a Cardano grid or variant of it, or by indication of punctuation marks on letters, syllables or words, which were widely used systems throughout the 19th and 20th centuries [7] (pp. 520–522).
- *Subliminal channel: substitution, insertion, and steganography.* In the same way, as in the previous case, it is a system already seen before, it being a composition of several systems. It was collated by Dunaynir himself, where sometimes the numbers that appeared in an astronomical text which referred to the number of celestial bodies, their rotations, positions, and other properties, were used to hide the literal substitutions of a certain message in their respective numbers or commercial and financial texts [42] (pp. 36, 46–47, 58, 140–141, 116–117).

We also find it in Tritemius, in which we have acrostic forms (insertions) with substitutions, as we can see that he made for the preparation of his "Steganographia", a book that hides a second book (the real one) inside [2] (pp. 283–287).
There is also the Porta-Guyot-Friderici musical system, which transformed the letters of the message into musical notes and sets of them, forcing the harmonization of the score, which is an insertion, as well as being a steganographic concealment system [33] (pp. 175–178).
Also included in this category is the substitution of the clear words of the message by others and placed in texts that are generally lengthy that deal with neutral issues, serving to mislead, using some type of grid to locate them—even being able to place themselves in a disorderly position, for which there would also be, in this case, transposition- or located in places indicated by punctuation marks or marks on the paper. As we can see, they are substitutions (and sometimes transpositions) and insertions, although the number of words inserted is generally greater than the number of words of the original message [7] (pp. 519–521).
An example of a pictorial nature is the graphic use of semagrams, that is, figures or iconic forms with meaning, which have close linguistic or numerical meaning, etc., within a larger drawing or graphic that hides the message in sight. It would be, for example, the use of binary codes, or Morse code, with the sketch of dots and stripes, or long and short stripes, in landscape graphics or any other, a technique which is sometimes called cryptoeidography [7] (pp. 522–523, 827–836, 989).

- *Insertion of nulls and nullifiers in the encrypted text, sometimes in the same encryption n-grams: substitution, insertion, and steganography.* Systems that, among others, used Tritemius, mixing null insertions in previous substitutions, are also present in his work "Steganographia" [2] (pp. 283–287). Additionally, there are various insertions of nulls and nullifiers (and the corresponding sequences to be canceled) in substitution ciphers generated by the nomenclator systems that sometimes had meanings of neutral themes and were alien to the true sense of the message they hid [7] (pp. 110–111).
- *Substitutions, elimination, and insertion.* This composition of encryptions is found already in the work of Ibrahim ibn Dunaynir, where together with monoalphabetic monographic substitutions and even the use of substitutions under the "hisab al-gummal" method, he eliminated some letters and even inserted nulls [42] (pp. 7–15, 28–36, 58, 76–82, 100–114, 126–140).
- *In general, any composition of methods in variable number and order.* Some examples that we find throughout the history of cryptography are outlined below.
  We start with the pioneering system of using substitutions of 1-g literals to {1, 2}-gram literals, with homophony and insertion of nulls, like that used by the Holy See created by Matteo Argenti in the year 1590 [3] (p. 55).
  Two centuries later we have the system of the Count of Mirabeau (1749–1791), which performs a Polybios substitution (from 1 to 5) and then a transposition of the coordinates taking all of the first ones and then all of the second ones, also adding null numbers (from 6 to 0), sometimes replacing the numerals to letters again [7] (p. 763).
  Another system is that devised by Pliny Earle Chase (1820–1886), in which after the substitution of letters from a rectangular 3 × 10 to numerical 2-g (x_i,y_i), it took the second coordinate under an operation (product by a constant, or sum of a constant, or even the logarithm), to pass the new values (x_i,y'_i) under the inverse of the 3 × 10 rectangular substitution to obtain the new letters [7] (pp. 203–204).
  Another illustrative example of the composition of three methods is that used in the Spanish–American War of the late 19th century, in which after the replacement of words or phrases through a codebook, another substitution of literal to numeral was made, to add a constant value to the result later [7] (p. 252).
  Or the ÜBCHI system, used by Germany before and during World War I, a polyalphabetical substitution after numerical assignment (bijective substitution), with subsequent transposition by numerical column ordering, followed by the addition of

nulls, and again transpositions, one of them horizontal and the other vertical [7] (pp. 301–304).

Also worth noting the complexity of compositions shown by liquor smuggling groups in the U.S.A. in 1920–1930, where substitutions of words to numbers were sometimes made from the codebook, followed by the addition of a constant number, with the same or another codebook to obtain subsequently a new word to which underwent a subsequent monoalphabetic substitution [7] (pp. 802–806).

Very similar to them was to replace the result of a numerical codebook first and then make various groupings of different sizes of n-grams, including transpositions, to do sums subsequently in a polyalphabetic way, very common systems during World War II by the Axis countries, Allies or neutral powers [7] (pp. 402–403, 440).

4. General Systematization of Cryptological Methods

The examples selected in the previous section serve as support for the algebraic section that follows. It was not our intention to mention all the existing examples that have arisen throughout history (but all methods and systems) or from all places and civilizations. However, we want to give some references that may be of interest to expand this matter, beyond those listed here. For example, ancient Indians [47,48] (ch. IV) [7] (p. 74), ancient Chinese [48] (ch. IV) [7] (pp . 73–74), Incas [49], ancient Eastern Christians [50], ancient Scandinavians [51], Arab world [52,53], Arab-African world [39,40], or the Ottomans [54], among the possible ones.

In the previous section, we showed a structure of methods according to a temporal and historical study of cryptology, offering the current classification which is commonly accepted today, at least in its section of classic cryptography, based on the two main systems, transposition, and substitution. To better structure it, we have added the arithmetic-algebraic functions to them, together with the methods of insertion and elimination, to later offer the various compositions of the previous methods.

Below we offer a more fundamental general scheme of cryptological methods, which we consider more broad and coherent, algebraically more compact, closed and complete, based on the wide range of the aforementioned methods.

4.1. The Elements

As we have seen, the elements of the initial and final sets can be very diverse. If we consider, in principle, linguistic texts for the initial message, we must consider their graphic elements or graphemes, or some of them, or parts, sequences, groupings, etc., depending on the encryption system that is applied. Thus, we can consider the vowels, the consonants, some specific letters, syllables, words, phrases, or any n-gram as a minimum block, and mixtures of any of these options.

Next to them, and for the possibilities of substitutions, should be considered any number or numerical form (on any numeral basis), be they Hindu-Arabic numerals or any other way of numbering (Romans, Cistercians, etc.). In addition, this applies to any letter of any alphabets, pure or mixed, punctuation marks and pseudo-forms derived from them, deformed, joining with each other, and so on, as well as alchemical, hermetic, astrological, tironian, geometric, musical, graphic signs, etc., and forms derived from them.

In short, any icon, symbol, even sound forms or phonemes, which we will generally call a gram, will be the various elements that we can consider in a general way in a cryptosystem as elements of the initial and final sets, which in general we can express as a finite set of elements of the set Σ, and that we will later see that we call X, Y, A, B, and later $\mathfrak{M}$, $\mathfrak{C}$ or $\mathfrak{K}$, depending on the context.

4.2. Substitutions

If we begin by analyzing the substitutions, so numerous and varied throughout history in their modalities, we must say that we cannot consider them in their algebraic sense, as some have pointed out, as functions, but as binary relations.

There is a binary relationship between two initial and final sets, X and Y, when at least $\exists x \in X/f(x) = y \in Y$, which, using the relationship notation, would be expressed as $\Re(x, y)$, or $x\Re y$, being $\Re$ the relation that makes them correspond.

Formally, the binary relation is defined as having previously defined the Cartesian product between X and Y, sets, $X \times Y$ as $\{(x, y)/x \in X \wedge y \in Y\}$. Thus, a binary relation $\Re$ on X and Y is a subset of $X \times Y$ where the relation $\Re$ is the one that corresponds to the encryption, $Enc()$, defining from $Y \times X = \{(y, x)/y \in Y \wedge x \in X\}$ the inverse relation in the same way, which we call decryption, $Dec()$.

In the binary relations, we have to differentiate the set of departure X, and the set of destination Y, the origin set A and the image set B. The origin set $A \subseteq X$ is made up of the elements of the departure set that have some relationship with the elements of Y, actually B. The image set $B \subseteq Y$ is made up of the elements of the destination set that have some relationship to elements of X, actually A.

Thus we would have:

- Non-unique binary relation: some element of the origin set A has more than one image.
- Univocal binary relation: each element of A has a single image.
- Biunivocal binary relation: each element of A has a single image and each image element of B has only one element of the origin set.
- Function: when all the elements of the departure set X have one and only one image.

A function is usually defined with two sets, D and C, domain and codomain. We say that f is a function from D to C, or that f is a map of D into C, written $f : D \to C$, if for each $x \in D$ there is a uniquely defined element $f(x) \in C$.

If we analyze the fundamental properties of functions, we have the following cases:

- We say that $f : D \to C$ is injective, or one-one, if for all $a, b \in D$, $f(a) = f(b)$ implies $a = b$.
- Likewise, f is surjective, or onto, if $f(D) = C$.
- If f is both injective and surjective, we say that f is bijective, or a one-to-one correspondence.

Sometimes we also talk about multivalued functions, which are not proper functions, but binary relations, when all the elements of the initial set have an image, although at least one of them has more than one.

By unifying all of the options, we see that these are defined, on the one hand, by the sets X, Y, and those that have an image by correspondence, by A and B, with the relation of strict inclusion or not, $A \subseteq X$ and $B \subseteq Y$; and, on the other hand, for the univocity in the origin set A, and the univocity in the image set B. There would be a total of 16 possible options, depending on the options {yes, no} to the conditions {$A = X$, $B = Y$, Uniqueness in A, Uniqueness in B}, which offer being {function/binary relation, surjective/non-surjective, non-multivalued/multivalued, injective/non-injective}. There are no more possible options.

These options are those that mark the possibility of homophonic encryption in the case of multivalued options; or polyphonic encryption in cases where the injectivity is not given. Although, to avoid ambiguities (which would be resolved during the decryption process and under the support of the language itself discarding possible semantic incongruities), it is more common that there is injectivity.

As for the other characteristics, which have to do with whether or not $A = X$ or $B = Y$ is fulfilled, the following is said: It is not necessary for encryption, but it may be common that the surjective or onto property is met ($B = Y$) and there are no elements in the image set that do not have an image, that is, elements $y \in B$ such that $\nexists Dec(y)$, although this aspect does not generate diversity in the type of encryption. As for the property that $A = X$ or not, we would be dealing with binary relations where at least some element of X had no image, that is, there was at least one value $x \in X/\nexists Enc(x)$, an aspect that does not generate distinctions in the various substitution encryptions.

That is why all possible cases of substitution would be included, the usual being that the bijective property is given, as occurs in the Gaius Iulius Caesar encryption, monoalphabetic, or the Vigenère, polyalphabetic.

We must add that even, in general, we should not talk about $f : A \to B$, but $f : A_1 \times A_2 \times \ldots \times A_n \to B_1 \times B_2 \times \ldots \times B_m$, and even, as binary relations: $\Re(A_1 \times A_2 \times \ldots \times A_n, B_1 \times B_2 \times \ldots \times B_m)$.

More specifically, what we find is the case $\Re(\mathfrak{M} \times \mathfrak{K}, \mathfrak{C})$, which, for example, we have in polyalphabetic ciphers, such as Vigenère-Belasso. On the other hand, monoalphabetic encryption can be expressed as $\Re(\mathfrak{M}, \mathfrak{C})$, because the key that is applied is always the same and can be taken for granted in the relation $\Re$, while in polyalphabetics it can occur, and in fact, it does occur, that $Enc(m_i, k_s) \neq Enc(m_i, k_t)$ when $k_s \neq k_t$, where $\mathfrak{M}$ is the message space, $\mathfrak{K}$ the key space, and $\mathfrak{C}$ the cipher space, constituent elements of the cryptosystem.

On the other hand, by virtue of the elements of the sets, our binary relations are discrete, therefore, the property of continuity does not exist.

With all the properties considered, and next to them, the composition of binary relations, we have completed all the possibilities that can be given, also showing the algebraic completeness of cryptographic options.

Finally, and considering in general that the various cryptographic systems are binary relations, where $\Re(\mathfrak{M}, \mathfrak{C})$ refers to an $Enc()$ binary relation, let us see if the reflexive, symmetric (or antisymmetric), and transitive properties are met:

- Reflexive ($a\Re a$). In general, it does not happen that $Enc(m_i, k_s) = m_i$. For the encryption property, the message or plaintext M must be different from the encrypted text C.
- Symmetric ($a\Re b \to b\Re a$). If $Enc(m_i, k) = c_i$, the original message does not have to be equal to the re-encryption of the encryption message, that is, in general, $Enc(c_i, k) \neq m_i$.
- Antisymmetric ($a\Re b \wedge b\Re a \to a = b$). If $Enc(m_i, k) = c_i$ and also $Enc(c_i, k) = m_i$, it does not necessarily force $m_i = c_i$. An example is the Atbash cipher (symmetric), which takes the specular letter within the Hebrew alphabet, so the antisymmetric property is generally not met.
- Transitive ($a\Re b \wedge b\Re c \to a\Re c$). In general, it does not happen if $Enc(m_1, k) = c_1$ and $Enc(c_1, k) = c_2$, it should be that $Enc(m_1, k) = c_2$.

Therefore, our binary relation $Enc(m_i, k) = c_i$, which we can express as $m_i\Re c_i \equiv Enc(m_i, k) = c_i$, for a given encryption using a key k, has neither a reflexive, symmetric, antisymmetric or transitive property, aspects that we can understand highly desirable for encryption.

In this way, the elements of an encryption–decryption scheme have already been defined: (Gen, Enc, Dec), where we only have to define the Generation function, Gen, which outputs a key k from the key space $\mathfrak{K}$.

4.3. Transpositions

Are transpositions a different group than substitutions? It seems that due to the huge number of cases and options shown for binary relations when analyzing substitutions, transpositions are not necessary.

It is clear that transpositions are bijective functions where $A = B$, which also algebraically identifies with permutations and applies to all elements or not, being able to analyze the diversity of existing algebraic cycles in them.

In the case in which the message to be encrypted did not have any repeated element, a bijective function $f : A \to A$ could be created, which made a certain new assignment, a permutation (of all the elements or only some), the result of this substitution coinciding with a transposition. Thus, if the message was $M = BYE$, and the substitution the following, defined by $f(B) = E$, $f(Y) = Y$, $f(E) = B$, the ciphertext $C = EYV$, so it is clear that it is a transposition that can be expressed as a substitution.

However, in the case in which some element of the message set appears more than once, there can be no coincidence between the substitution (which in that case will require two different elements) and the transposition. Thus, in the following example, where $M = GOOD$, the substitution being as follows, we force it to be a transposition, $f(G) = O$, $f(O) = D$, $f(O) = O$, $f(D) = G$, the ciphertext is $C = ODOG$. We see that there will always be two equal values in origin set, the letter O, which has different images. This makes the transposition no longer a function, it is more, it is not a bijection, and we cannot say that the substitution of the letter O is a single letter because there is polyphony.

Therefore, to achieve unification, the set of keys $\mathfrak{K}$ is required, and in this way, in general, transpositions are substitutions, but polyalphabetic, $\Re(\mathfrak{M} \times \mathfrak{K}, \mathfrak{C})$, where, through the different values of k_i, we get the desired c_i value of the transposition. Thus, in the previous example, if $M = GOOD$, giving the key sequence to be added under the Vigenère-Belasso system $K = XSAL$, we would have a value $C = DGOO$, a transposition.

Consequently, given a message $M = m_1 m_2 \dots m_i \dots m_i \dots m_j$, and if any transposition is desired as ciphertext $C = m_q m_i \dots m_j \dots m_i \dots m_n$, it is always possible to find the appropriate value of $K = k_s \dots k_d \dots k_w \dots k_p$, that added member-by-member gives the expected result.

Therefore, transpositions cannot, in general, be defined as substitutions except when the Cartesian extension $\Re(\mathfrak{M} \times \mathfrak{K}, \mathfrak{C})$ is taken, which means that the same element m_i no longer exists, in particular, more than once, but two different elements, (m_i, k_f) and (m_i, k_r), which give the desired value, not necessarily the same, in the encrypted set $\mathfrak{C}$, according to the desired transformation; likewise, two possible values (m_j, k_b) and (m_m, k_e), can have the same image in $\mathfrak{C}$. In this way, we can define transpositions as bijective functions.

For all of these reasons, and because the analysis carried out on the binary relations has been a complete study of all possible options, the permutations of set A on itself, the transpositions must remain within it, although it requires us to consider all the elements of the message M at the same time to match the ciphertext C, carefully choosing the various values of the key K. This is the singularity of transpositions, in which the whole message and all of the elements in them, must be considered at the same time, which does not occur with substitutions, as we have seen in the various methods and systems over time. In this way, they are binary relations, in which it is necessary to know all the elements of the plaintext, the message, to build the various keys k_i, and the context is necessary for the complete sequence that must be encrypted. It is not simply a replacement element after element. Therefore, transpositions take into account the entire sequence to be permuted, which, we would say, is not the case with the more "genuine" substitutions.

4.4. Generalizing Substitution and Transposition

Let us clarify the previous aspects a little more with the following generalization of both procedures, substitutions, and transpositions.

If we consider a certain message M to be encrypted, which is made up of discrete elements, and which form an orderly sequence of its elementary units, for example, $m_1 m_2 m_3 \dots m_n$, on each element m_i only two operations can be performed $\{G_1, G_2\}$, taking into account that we cannot consider more than one element (which would be subject to an assembly of elements or a segmentation), nor eliminate it, nor add another, nor use G_1 once and other times G_2 (which would be object of composition of binary relations). With this, the two operations that can occur are:

- G_1, consisting of taking m_i and putting another element of the sequence $m_1 m_2 m_3 \dots m_n$ (or itself, which would leave it the same) in its place, interchangeably.
- G_2, consisting of taking m_i and putting another element, not taken from the sequence $m_1 m_2 m_3 \dots m_n$ in its place (or not, leaving it as it is). It would, however, take it, changed, from another set, whatever it may be, that may have the same elements as the sequence (or not).

There are no more options than these. Operation G_1 is a transposition, and operation G_2 is a substitution. It is clear that both options are disjointed (although sometimes, as we saw before, they can lead to the same results, which is a different matter) and both form a complete and closed set of options on the sequence $M = m_1 m_2 m_3 \ldots m_n$.

The operation that encompasses the set of G_1 and G_2 will be called the *Get* operation, $\mathfrak{G}$, where $\mathfrak{G}$ is the set that includes all transpositions ($\mathfrak{t}$) and all substitutions ($\mathfrak{s}$), since $G_1 \equiv \mathfrak{t}$ and $G_2 \equiv \mathfrak{s}$, hence $\mathfrak{G} = \mathfrak{t} \cup \mathfrak{s}$.

4.5. Arithmetic-Algebraic-Logical Operations

Throughout history, we have also seen some ciphers that used methods based on simple operations, especially arithmetical operations, such as sum or product (successive sums) and their respective inverses, either integer or modular operations. Or the repetition of products, that is, the exponential, present in the current asymmetric ciphers. To them, we must add the logical operations, which we can find especially from the DES cipher. We have to say that logical operations are arithmetical Boolean operations with the inverse element, and these with arithmetic are a subset of the algebraic ones. In short, it is any algebraic operation, however complicated it may be, as well as all its possible combinations and joint use.

However, all of them are examples of substitutions, after assigning the initial elements of the set to numerals, however complicated they may seem or really be, whether they are arithmetic operations such as sum or product, modular exponentiation or product, operations with polynomials, or product operations with points of geometric curves, summarizing operations within an algebraic group.

4.6. Pre-Cryptological Operations

Apart from the cryptological operations of the *Get* set $\mathfrak{G} = \mathfrak{t} \cup \mathfrak{s}$, we have to consider other different operations, which serve as an aid in the information masking process, which we call pre-cryptological operations, being related to the linguistic properties of the message itself. In total there are four procedures, dual two-to-two, which have to do with the sequence of the message. On the one hand, Insert and Delete, which have to do with the inclusion or exclusion of elements; and on the other, Join and Segment, which have to do with the unification or fragmentation of the message sequence.

4.6.1. Insert and Delete

The message $M = m_1 m_2 m_3 \ldots m_n$ can be considered as an ordered sequence of elements. Hence, we can consider two basic operations, which are dual of each other, the insertion and elimination of elements.

These aspects, prior to any cryptographic action, refer to the language of the message itself, introducing spurious elements to the plaintext, or removing the capacity for redundancy in the language, which could lead to altering the initial sequence.

In a formal and abstract way, we can consider the message as an ordered n-dimensional vector within a vector space, $(m_1, m_2, m_3, \ldots, m_n) = \overrightarrow{M}$. In this way, we define these operations as:

- Insert (Ins_i): This increases the vector space dimension in the new coordinate i.
- Delete (Del_i): This removes one dimension, the coordinate i, from the vector space.

It is clear that the repetition of Insert increases or expands the initial vector $M = m_1 m_2 m_3 \ldots m_n \equiv (m_1, m_2, m_3, \ldots, m_n) = \overrightarrow{M}$ as much as desired. In the same way, the repetition of Delete eliminates until all of the initial vector $\overrightarrow{M}$ disappears or is eliminated. Thus, the composition of Insert is another function of insertion and the composition of Delete is another elimination.

The process of dimensional expansion Insert, for example, of a new element, m_w, increasing the dimension, after m_{i-1}, $Ins_i^{m_w}(\overrightarrow{M})$, can be seen as the step from

$$(m_1, m_2, \ldots, m_{i-1}, m_i, m_{i+1}, \ldots, m_n) \textit{ to } (m_1, m_2, \ldots, m_{i-1}, m_w, m_i, m_{i+1}, \ldots, m_n).$$

This is expressed with matrices by doing

$$(m_1, \ldots, m_{i-1}, m_i, \ldots m_n)\begin{pmatrix} 1 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & \ldots & 1 & 0 & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & \ldots & 0 & 0 & 0 & \ldots & 1 \end{pmatrix} = (m_1, \ldots, m_{i-1}, 0, m_i, \ldots m_n).$$

Afterwards, without forgetting that the value 0 in this representation is not properly a sign of the set of elements $\mathfrak{M}$, but a null (empty) value, but that already allows it to be used as an indication of a new dimension of the previous vector space, it reaches the sum

$$(m_1, \ldots, m_{i-1}, 0, m_i, \ldots m_n) + (0, \ldots, 0, m_w, 0, \ldots, 0) = (m_1, \ldots, m_{i-1}, m_w, m_i, \ldots m_n).$$

For its part, the process of dimensional compression or Delete eliminates a certain value, for example, m_i, $Del_i(\overrightarrow{M})$, passing from

$$(m_1, \ldots, m_{i-1}, m_i, \ldots, m_n) \textit{ to } (m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n).$$

Using matrices, as in the case of vector spaces, the procedure of eliminating the respective dimension would be to multiply by a $n \times n - 1$ matrix, with a row of zeros in the place we wish to remove:

$$(m_1, \ldots, m_{i-1}, m_i, \ldots m_n)\begin{pmatrix} 1 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & \ldots & 1 & \ldots & 0 \\ 0 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & \ldots & 0 & \ldots & 1 \end{pmatrix} = (m_1, \ldots, m_{i-1}, \ldots m_n).$$

Let us indicate that due to the intrinsic property of $Del_i(\overrightarrow{M})$, insertion and elimination are not inverse operations since it is true that $Del_i(Ins_i^{m_w}(\overrightarrow{M})) = \overrightarrow{M}$, we have $Ins_i^{\alpha}(Del_i(\overrightarrow{M})) \neq \overrightarrow{M}$, since the value lost in the elimination that would have to be inserted to recover it is unknown because the elimination operation implies a loss of message information. It is for this reason that this operation is not usual, much less especially in repeated compositions of operations, as it may entail not being able to recover the original message in decryption.

4.6.2. Join and Segment

The sequence of elements, discrete elements, of the message M to be encrypted can be seen as a sequence in a "geometric" sense, hence we can split it into pieces, an aspect that we will now try to explain through two functions, one of segmentation, and its dual, of unification.

As we have seen in the previous historical subsection, the sequence of elements to be encrypted, although constituted many times by minimum units, these grams are grouped with adjacent ones, in greater or lesser lengths, forming units of different sizes, and with it, generating new elementary units. Even, and by the use of bijective substitutions or encodings, they are previously passed from one set of elements to another to be able to make these new groupings.

We will clarify it with the following example. Thus, a message $M = CRYPTO$, with an assignment of letters to numbers such as the following, which is a bijection, $C \rightarrow 832$, $R \rightarrow 52$, $Y \rightarrow 713$, $P \rightarrow 30$, $T \rightarrow 681$, $O \rightarrow 46$, becomes the ciphertext $M_1 = 832, 52, 713, 30, 681, 46$, and if blocks of 4 elements (4-g) are now taken, adding character 5 if required, as many times as necessary, at the end, our result would remain as $M_2 = 8325, 2713, 3068, 1465$.

As we can see, we have transformed a set of elements, Latin-Western letters, into numeral blocks, $\{0 \ldots 9\}^4$. It is an operation consisting of the change from one universe of elements to another, whichever universes of elements we consider.

It is an operation that on many occasions is very common in cryptography, very generally at the beginning of the cryptographic process, although, due to the composition of transpositions and substitutions, it is also interleaved or even applied at the end of the total encryption process.

The coding operation, as seen in the example above, would be a previously analyzed substitution. However, the subsequent one is an operation not seen until now nor formalized. We will define it as Segment (Sg), due to its geometric similarity with the application of a certain measure on the sequence of elements. Yet we also need to define another operation, Join (Jn).

- Join (Jn): Given a set $U = \{u_1, u_2, u_3, \ldots, u_n\}$, if we have any sequence $M = u_j, u_t, u_s, \ldots u_t$, Join eliminates the discretization of the elements of the set U: $Jn(u_j, u_t, u_s, \ldots u_t) = u_j u_t u_s \ldots u_t$. In this way Join makes you lose the individuality of the initial elements, and thus, generates a unified sequentiality without the distinction of discrete elements.
- Segment (Sg): Given a continuous sequence, such as that obtained through the Jn operation, from the segmentation operation specifications, Sg divides and splits the sequence into individual units, which will be elements of a set of W elements. Segmentation can be done in blocks of equal length or not, and you must specify the values to be added (if necessary) to the source sequence at its end.
  In general, we can define it as
  $$Sg^{W_1, W_2, \ldots, W_s}_{\omega_1, \ldots, \omega_t}(u_j u_t u_s \ldots u_t) = w^1_g, w^2_d, w^3_h, \ldots, w^s_m, w^1_r, \ldots, w^i_l, \omega_1 \ldots \omega_j,$$
  where the different $W_i = \{e_1, e_2, \ldots, e_j\}^r$ sets of elements made up of their minimum units from which we will take r from them. The different ω_i are the values that will have to be appended at the end of the sequence so that the last block has the appropriate length that marks its respective set W_t.

With all this, returning to our previous example, $Jn(M_1) = 832527133068146$. Then applying $Sg(832527133068146)$ on a set $W = \{0 \ldots 9\}^4$ and $\omega = 5$ as the final addition, we can express it as

$$Sg^{W=\{0\ldots 9\}^4}_{\omega=5}(832527133068146) = 8325, 2713, 3068, 1465.$$

The use of the functions Jn and Sg are quasi-inverse of each other, due to the insertion of the elements taken from $\omega_1, \ldots, \omega_t$, and M being the sequence to be encrypted into any set of elements, be they numbers, letters, any symbol, pictogram, graphic, even image, audio, etc. (Let us keep in mind that during World War II, the German, Japanese, or American armies used, both in the temporal and frequency domain, transpositions of audio fragments of a conversation or sub-band substitutions [7] (pp. 549–560)), allowed all the cryptographic procedures of the set Get to be applied, $\mathfrak{G} = \mathfrak{t} \cup \mathfrak{s}$, as well as the functions Ins_i and Del_i to any object or element that we can consider.

4.7. Composition of Binary Relations

Cryptological and pre-cryptological operations can be made up between them, generating the diversity of options that we have found throughout the history of cryptography, and all that are possible, these being complete and closed sets: on the one hand, any type possible of binary relation, with the diversity of options of the *Get* operation, $\{\mathfrak{s}, \mathfrak{t}\}$, and on the other hand, the options on the sequence of elements, $\{Sg, Jn\}$ and $\{Ins, Del\}$.

We can talk about internal compositions when the composition is applied to the same type of these six operations or otherwise external compositions. Thus, the composition of transpositions is a transposition; the composition of substitutions is a substitution; the composition of insertions is a sequence of insertions; the composition of eliminations is a sequence of eliminations; the composition of segmentations is a segmentation; and in the case of Join, it makes no sense to make it up with itself, repeatedly, as the result is similar to that of the first application of the operation.

The composition is used to achieve another cryptographic system that could not be achieved with the individual systems used in the composition, and that is more secure.

It is the mixture of these compositions that offers the best results to increase security, so that the repeated composition (what is known as rounds) of transpositions (aspect of diffusion) with substitutions (aspect of confusion), and next to them the use of pre-cryptological operations increases the cryptanalytic difficulty of attacking the cryptological system and the effort or work against it.

5. Some Clarifications and Explanations

After having offered a more compact and complete algebraic scheme of crypto methodology, we will briefly comment on some aspects of perfect and ideal encryption, as well as the divisions on block and stream ciphers, and symmetric and asymmetric ciphers.

5.1. Perfect Encryption and Ideal Encryption

After fully studying the cryptological and pre-cryptological operations, we can make some additional comments.

Due to the distinction between transposition and substitution operations, the concepts linked to them of confusion and diffusion are differentiated, as they were considered and defined by Claude E. Shannon [22], and Horst Feistel reiterated them [55], making use of the mixing of both transformations (composition of binary relations), not being subsumed if the transpositions were substitutions, the concept of diffusion (linked to transpositions) into the concept of confusion (linked to substitutions).

On the other hand, we can talk about perfect secret, and with it, about perfect encryption in confusion and diffusion, the perfect encryption is the one in which $Pr(M = x/C = y) = Pr(M = x)$, i.e., the probability *a posteriori* that the original text is x if the ciphertext is y, is identical to the probability *a priori* that the original text is x. When considering the entropy, uncertainty or equivocation, $H(M/C) = H(M)$. The ciphering does not give any information. Therefore, the mutual information of the message and the ciphertext, $I(M, C) = 0$. Thus, considering entropy or uncertainty, $H(M, C) = H(M) + H(C)$, so it is also true that $H(C/M) = H(C)$. Perfect encryption in both substitution and transposition applied to the message sequence $M = m_1 m_2 m_3 \ldots m_n$ makes every m_i element a perfect substitution (Vernam encryption), which can be seen as that element having been replaced by another c_i taken under a completely random process, that is, without any relation to m_i, and thus with the entire sequence. Thus, perfect confusion is achieved. On the other hand, a perfect transposition (different from perfect encryption, which would also require the number of keys to equal the number of messages) would mean that in each position between $\{1, 2, \ldots, n\}$ of the sequence of elements, each one has been placed in an ordinal place randomly, so there is no relationship between its new placement and the one in the original sequence $M = m_1 m_2 m_3 \ldots m_n$. Similarly, we can call it perfect diffusion.

Cryptographic binary relations and their compositions together with the use of the methods we call pre-cryptological focus on the properties of language, allow the linguistic properties to be altered, achieving greater system security, as well as the ideal secret.

Calculating the unicity distance, which gives us the value of the length of the text when the spurious keys tend to 0, this is given by $n_0 \approx \frac{\log_2 |\mathfrak{K}|}{R_L \log_2 |\mathfrak{M}|}$, R_L being the language redundancy, defined by $R_L = 1 - \frac{H_L}{\log_2 |\mathfrak{M}|}$, where H_L is the language entropy, which is defined as $\lim_{n\to\infty} \frac{H(\mathfrak{M}^n)}{n}$, the preceding dividend being the entropy of a message of length n. Therefore, using the aforementioned pre-cryptological operations, we can eliminate all redundancy, leading to no relationship between the various characters of the message to be encrypted, achieving total independence of the message's grams, there being no correlation, resulting in $H_L = \log_2 |\mathfrak{M}|$, so $R_L = 0$ and n_0 tends to infinity.

We are then in the case in which the equivocation of the key and the message do not approach zero although the message tends to infinity, fulfilling the ideal encryption condition, and also, as the equivocation of the key, which is equal to the entropy of the key, $H(\mathfrak{K}) = \log_2 |\mathfrak{K}| = c$, constant, we have strongly ideal encryption, according to Shannon. In this way, it does not matter how much encrypted material you have, even $n \to \infty$, that a single solution of the original message cannot be known, the $Work$ ($\mathfrak{W}$) necessary to solve the encryption is also tending to infinity. Thus, in this case, there is the situation in which the ciphertext and the key are mutually independent, $I(K, C) = 0$, so considering the equivocation, $H(K/C) = H(K)$, and $H(C/K) = H(C)$.

5.2. Block Ciphers and Stream Ciphers

Sometimes we talk about block ciphers (DES, AES, IDEA, FEAL, SAFER, RC5, etc.) and stream ciphers, but this is not a very useful classification and without algebraic distinction. By virtue of our Join and Segment operations, the origin elements of the encryption can have different lengths, from 1 to more than 1 element, thus formalizing this differentiation.

Block ciphers can be analyzed in their components as composite structures of the different cryptological and pre-cryptological operations [31] (pp. 265–368). Thus, if we review the two best-known and used contemporary block ciphers, although something similar could be done with the others, we can see how they can be included within the methods analyzed.

- *DES encryption.* For the "Data Encryption Standard" (DES) symmetric encryption [56], the constituent elements of encryption (similarly to decryption) are: Starting with the substitutions of the message literals for their binary encodings at the beginning and end of the process (substitution), we find permutation IP operation and their inverse (transposition), expansion (insertion), $S-box$ (substitution with polyphony), permutation P (transposition), $PC1$ and $PC2$ for subkeys (transposition), shifts (transposition) and XOR functions and modular sums (arithmetic-algebraic-logical functions). With them we also find the Feistel structure, with its Sg and Jn operations and the various rounds or replications of the entire set of operations (external composition of binary relations).
- *AES encryption.* In the symmetric encryption "Advanced Encryption Standard" (AES) [57], the constituent elements of encryption (similarly to decryption) are: Starting with initial substitutions of the message literals to their binary encodings at the beginning and end of the process (substitution), and the various Sg and Jn that mark the structure of the $GF(2^8)$ and the Word of $GF(2^{32})$, we find $SubBytes$ or $S-box$ (substitution), $ShiftRows$ (transposition), $MixColumns$ (substitution), block rearrangement (transposition), $AddRoundKey$ or modular sums (arithmetic-algebraic-logical functions), $Rotate$ or shifts (transposition), $Rcon$ or $S-box$ (substitution), $SubWord$ or $S-box$ (substitutions), $RotWord$ (transposition), and XOR functions and modular sums (arithmetic-algebraic-logical functions), as well as the various rounds or replications of the whole set of operations (external composition of binary relations).

As for the stream ciphers [31] (pp. 369–428), all of them, such as A5/1, A5/2, RC4, Salsa20/12, Sosemanuk or Trivium, and before them from the Vigenère-Belasso method to the Vernam one-time-pad (maximum random key without periodicity), they aim to achieve keys as random as possible, in general using Linear Feedback Shift Registers (LFSR) or Nonlinear FSR, but also Feedback with Carry Shift Registers (FCSRs), which are still arithmetic-algebraic-logical operations, although sometimes they use other types of operations, such as SEAL or Rabbit: arithmetic-algebraic-logical operations, transpositions, substitutions, and pre-cryptological operations Sg and Jn. On the other hand, and considering that asymmetric ciphers are variants of symmetric ones with a trap-door, there are also asymmetric stream ciphers, such as Blum–Goldwasser, by joining the problem of Integer

Factorization and Modular Square Roots, with the pseudo-random number generator BBS (Blum Blum Shub), thus being probabilistic.

5.3. Symmetric and Asymmetric Ciphers

Encryption performs the operation $Enc_k(m) = c$, for certain $m \in M$ and $c \in C$, and a key $k \in K$, so that decryption allows the original message to be obtained again $Dec_k(c) = m$.

It is clear that the encryption process, for whatever system, uses the value of the key k. That is why to decipher you have to use the same key, k. However, it is not used in the "same way", as the process of encryption is not usually performed in the "same way" as that of deciphering. The truth is that there is an inverse similarity between the two, being able to express that $Enc = Dec^{-1}$ and that $Dec = Enc^{-1}$. The decryption operation applies the same steps in ciphertext as in encryption, albeit "backwards", we could say.

Thus, if the encryption operation is a sum, the decryption process will be a subtraction. Or in general, if the binary relation when dealing with substitutions is from the set X to Y, in the decryption it will be from the set Y to X. In the case of transpositions, the original element will be taken for each permuted element and returned to where it was initially located.

Similarly, we can talk about reversing the pre-cryptological processes Ins, Del, Jn, Sg. We can also apply the different compositions of binary relations in the opposite direction.

With all this, it is understandable that until 1976, when Whitfield Diffie and Martin Hellman's paper "New Directions in Cryptography" was written [13], cryptography was considered as symmetric, where the encryption key is the same (in the exposed sense) as the decryption key.

From that moment, we began talking about another type of cryptography, asymmetric. However, it maintains the same characteristics as any encryption, but where some aspects of the key are not known to everyone. Let us explain it with two of the best-known asymmetric ciphers:

In the Elgamal cipher [15] (pp. 294–298), if we consider it as symmetric encryption, the encrypted message, from the plaintext message m, is $c = mg^{ab}$, value within $\mathbb{Z}_p$, and the key would be $k = g^{ab}\ mod\ p$. It would be a modular multiplication in $\mathbb{Z}_p$. In order to decipher it, the inverse operation in the multiplicative group $\mathbb{Z}_p$ would be applied, specifically, $cg^{-ab} = mg^{ab}g^{-ab} = m$. However, we can give some asymmetry in the process, which is what we call asymmetric encryption if we express the key $k = g^{ab}\ mod\ p$ as $k = (g^a)^b\ mod\ p$. Knowing the value $g^{ab}\ mod\ p$ is not computationally easy to obtain the exponent b even if the value $g^a\ mod\ p$ is known, which is known as the Discrete Logarithm Problem, allows us to divide or split the key, or put another way, hide aspects of the key, specifically the exponent b. With this, an actor or part of the communicative process (who knows $\{a, g^b\}$) encrypts it by multiplying the message m by $(g^b)^a$, and the other part (who knows $\{b, g^a\}$) deciphers it by applying division by $(g^a)^b$.

For RSA encryption, supported by the Integer Factorization Problem, and the RSA Inversion Problem, the situation is similar [15] (pp. 285–291). Here the encrypted message is $c = m^e\ mod\ pq$, value within $\mathbb{Z}_{n=pq}$, and the key would be $k = e\ mod\ \varphi(n)$, where $\varphi(n) = (p-1)(q-1)$. Decryption is the inverse operation, which means dividing by k or multiplying by $k^{-1} = e^{-1}\ mod\ \varphi(n) = d\ mod\ \varphi(n)$. In this case, the asymmetry of the encryption with the decryption is that given e it is not possible to obtain d if Euler's function $\varphi(n)$ is unknown. For this reason, it seems that there are two keys, but they are really the same, to be applied directly to encrypt or vice versa to decrypt. Yet because $\varphi(n)$ is not offered publicly, even if we have e, we cannot obtain $d = e^{-1}\ mod\ \varphi(n)$, because of the computational problems on which RSA rests, hence it seems that there are two different keys.

Something similar can be applied to the rest of the asymmetric ciphers. This is done by the same constitution of encryption and decryption operations in which $Enc = Dec^{-1}$ and $Dec = Enc^{-1}$, and which we can express as $Enc_k = Dec^{-1}_{k^{-1}}$ and $Dec_{k^{-1}} = Enc^{-1}_k$. Therefore, asymmetric encryption can always be generated if there is a relationship between k and k^{-1} which is not easy to achieve (computationally speaking, as a mathematical complexity problem), due to a restriction of information, based on symmetric encryption (or just encryption), which is always the basis of any encryption. Hence, even the most complex symmetric ciphers, such as DES or AES, offer in their decryption a sequencing of reverse steps to those carried out in the encryption by applying the subkeys in the reverse order, to obtain $Dec_k(c) = m$.

This is known as "trapdoor", where there is additional and secret information, capable of carrying out the reverse operation. If this information did not exist, we would talk about a one-way function, more generally, according to our algebraic structure, one-way binary relation.

These trapdoors are built based on computationally hard problems. Some computational problems of cryptographic relevance are: Integer Factorization (IFP), RSA Inversion (RSAIP), Quadratic Residuosity (QRP), Modular Square Roots (MSRP), Multivariate Quadratic Equations (MQEP), Discrete Logarithm (DLP) and its Generalization (GDLP), Diffie-Hellman (DHP) and its Generalization (GDHP), Subset Sum (SSP), Linear Code Decoding (LCDP), Shortest Vector in a Lattice (SVP), Learning With Errors (LWEP).

To name but a few of the main encryption schemes, we have: RSA encryption relies on IFP and RSAIP; Rabin on IFP and MSRP; McEliece on LCDP; Merkle–Hellman Knapsack on SSP; Elgamal and Cramer–Shoup rely on DLP and DHP; Elliptical Curves on GDLP and GDHP; Goldwasser–Micali on QRP; Hidden Field Equations (HFE) rests on MQEP; NTRU-Encrypt on SVP; Fully Homomorphic Encryption of Brakerski–Gentry–Vaikuntanathan (FHE-BGV) rests on LWEP.

Thus, all of them are based on the same principle. Even some more peculiar encryption schemes such as Goldwasser–Micali operate bit-by-bit with pseudo-random values (in the manner of a key sequence) to generate a semantically secure probabilistic encryption with trapdoor. Blum–Goldwasser is also semantically secure and probabilistic with trapdoor and key sequence for the different n-grams of the message based on the BBS pseudo-random generator.

That is why we call the ciphers asymmetric—if all their elements were given, they could be used as completely symmetric ciphers. However, due to their slowness (since they use mathematical operations of greater computational effort than in symmetric ciphers) it would not make much sense, although in case it was needed because secure ciphers were not available, due to attacks on AES, T-DES, and others, such as Twofish or Serpent, asymmetric ones could be used symmetrically.

Moreover, considering that all ciphers are essentially in the form $Enc_k(m) = c$ and $Dec_k(c) = m$, whether or not they have a pair of keys $\{k, k^{-1}\}$, it is more or less simple to obtain one from the other; the ciphers that we have mentioned here and that are commonly called asymmetric are, from the perspective of their algebraic foundation, substitutions, so in essence they are not too complex, neither usually presenting in their structure transpositions nor the composition of binary relations nor pre-cryptological operations, operating the substitutions under the application of various mathematical operations in an algebraic group, be they the elements of $\mathbb{Z}_p$, $\mathbb{Z}_n$, $\mathbb{Z}_{n^2}$, $\mathbb{F}_{2^m}$, or the points of an elliptic curve $E(\mathbb{F})$, a vector subspace $\mathbb{F}_q^n$, a polynomial ring $\mathbb{F}_q[X]$, a truncated polynomial ring $\mathbb{Z}[X]/(X^N - 1)$, or any other, resting its strength and security on computational properties and problems which are difficult to solve.

6. Conclusions

This work is essentially mathematical, and it is not a historical paper, much less a survey. The diversity of systems exposed here has only been collected as examples to better understand the subsequent categorization that we offer. They serve us in their completeness as support for the later algebraic section.

Hence after collecting with a sufficient range the diversity of cryptographic methods and systems, with an abundance of examples, which have emerged during the long course of the history of Cryptology, we wanted to offer one first ordering of them based on the usual organizational structure, which subdivides them into transposition and substitution ciphers.

We have added elimination and insertion operations, which we also find disseminated in the history of ciphers, and which are barely taken into account, and to which we will then give a necessary and complete sense; in addition, in our first arrangement, we collected the mathematical operations and compositions of operations.

From this material, we propose a classification of cryptological methods and systems. Although we can find many mentions of function, bijection, injection, and other concepts, in various authors, until now, that we know of, such a complete and compact one has not been offered. The novelty is not in the concepts used but in their use, in order to give a categorization of cryptological methods and systems.

This framework, with its various properties and options, allows the entire field of cryptology to be completely restored and visualized, allowing us to understand its methodological diversity.

In addition, it has allowed us to offer a better characterization of transposition and substitution operations, which we have placed under the diversity of binary relations. In addition, we have joined them together under the *Get* set, a set of cryptological operations, with no other option than the two, thus being a complete and closed set.

We have completed the operational set with four operations that we call pre-cryptological, not being part of the *Get* set of transpositions and substitutions. They arise from the approach to the sequence of elements of our departure and destination sets from a vision close to Geometry since if we consider them as discrete units, by their own sequentiality, we can apply them to operations of adding or removing, on the one hand; and union or fragmentation operations. They are, respectively, the Insert and Delete operations, for the first couple, and the Join and Segment operations for the second. Both groups are complete in all their operations. Pre-cryptological operations are directly related to linguistic properties and are necessary for the cryptographic process of information concealment.

This entire framework of pre-cryptological and cryptological operations, and its various compositions, which we apply to any possible element, allows us to visualize all the possibilities and finally understand the reason and the location of transposition, substitution, homophony, polyphony, monoalphabetism, polyalphabetism, monograms, and polygrams, as well as the nomenclator, or the nulls and nullifiers, the mathematical operations (arithmetic-algebraic-logical operations), so common in modern systems, etc., and that only acquire their full meaning when seeing them under the prism of binary relations.

All this also allows us to better understand the meaning of perfect ciphers and ideal ciphers. Along with it, we can also specify in its most appropriate sense the distinctions, which we can take as surpassed, between symmetric and asymmetric ciphers, and also between block and stream ciphers.

The algebraic perspective offered here also allows a reading of the categorized systems from the viewpoint of computational or algorithmic number theory. It also helps when choosing the various cryptanalytical methods when attacking different systems.

The encryption/decryption systems are applied to any message, regardless of its type, be it text, audio, video, etc., once it has been digitally encoded. The modality of its structure in the communication and transmission process, for example, in IP packets, does not alter the classification we offer either. The same can be said of structures such as the blockchain, which uses the usual cryptographic methods. Neither does post-quantum cryptography modify our categorization. Thus, ciphers such as McEliece, NTRU, or Merkle signature scheme, respectively linked to code-based, lattice-based, or hash-based algorithms, or other post-quantum modalities, can be placed in the different methods and systems that we give.

We hope we have managed to establish and formalize the algebraic statute better, and therefore, the fully mathematical side of cryptological science.

Author Contributions: Conceptualization, V.J.-V. Funding Acquisition, C.S.-Á. Methodology, V.J.-V. Investigation, V.J.-V. Supervision, V.J.-V. and C.S.-Á. Validation, V.J.-V., Carmen C.S.-Á. Writing, V.J.-V. All authors have read and agreed to the published version of the manuscript.

Funding: This study has received support from the Instituto Nacional de Ciberseguridad (INCIBE), from Ministerio de Economía y Empresa of Spain, within the framework of the "Ayudas para la excelencia de los equipos de investigación avanzada en ciberseguridad" (ref INCIBEI-2015–27342).

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Leighton, A.C. Secret Communication among the Greeks and Romans. *Technol. Cult.* **1969**, *10*, 149–152. [CrossRef]
2. Strasser, G.F. The Rise of Cryptology in the European Renaissance. In *The History of Information Security: A Comprehensive Handbook*; de Leeuw, K., Bergstram, J., Eds.; Elsevier: Amsterdam, The Netherlands, 2007; pp. 277–325.
3. Bauer, F.L. *Decrypted Secrets: Methods and Maxims of Cryptology*; Springer: Berlin, Germany, 2007.
4. Muñoz Muñoz, A.; Ramió Aguirre, J. *Cifrado de las Comunicaciones Digitales. De la Cifra Clásica al Algoritmo RSA*; 0xWord: Madrid, Spain, 2019.
5. Galende Díaz, J.C. *Criptografía: Historia de la Escritura Cifrada*; Editorial Complutense: Madrid, Spain, 1995.
6. Dooley, J.F. *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*; Springer: Cham, Switzerland, 2018.
7. Kahn, D. *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*; Scribner: New York, NY, USA, 1996.
8. Singh, S. *Los Códigos Secretos*; Debate: Madrid, Spain, 2000.
9. Bauer, F.L. Rotor Machines and Bombes. In *The History of Information Security: A Comprehensive Handbook*; de Leeuw, K., Bergstram, J., Eds.; Elsevier: Amsterdam, The Netherlands, 2007; pp. 381–446.
10. Frik, S. Boris Hagelin and Crypto AG: Pioneers of Encryption. In *The History of Information Security: A Comprehensive Handbook*; de Leeuw, K., Bergstram, J., Eds.; Elsevier: Amsterdam, The Netherlands, 2007; pp. 479–496.
11. Klein, M. *Securing Record Communications: The TSEC/KW-26*; CreateSpace Independent Publishing Platform: Scotts Valley, CA, USA, 2012.
12. Bauer, C.P. *Secret History: The Story of Cryptology*; CRC Press: Boca Raton, FL, USA, 2013.
13. Diffie, W.; Hellman, M. New Directions in Cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
14. Merkle, R. *Secrecy, Authentication, and Public Key Systems*; UMI Research Press: Ann Arbor, MI, USA, 1979.
15. Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1997.
16. Cohen, H.; Frey, G.; Avanzi, R.; Doche, C.; Lange, T.; Nguyen, K.; Vercauteren, F. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*; Chapman & Hall/CRC: Boca Raton, FL, USA, 2006.
17. Buchmann, J.A.; Butin, D.; Göpfert, F.; Petzoldt, A. Post-Quantum Cryptography: State of the Art. In *The New Codebreakers. Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*; Ryan, P.Y.A., Naccache, D., Quisquater, J.J., Eds.; Springer: Luxembourg; Paris, France; Louvain-la-Neuve, Belgium, 2016; Volume 9100, pp. 88–108.
18. Desmedt, Y. What is the Future of Cryptography? In *The New Codebreakers. Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*; Ryan, P.Y.A., Naccache, D., Quisquater, J.J., Eds.; Springer: Luxembourg; Paris, France; Louvain-la-Neuve, Belgium, 2016; Volume 9100, pp. 109–122.
19. Preneel, B. An Introduction to Modern Cryptology. In *The History of Information Security: A Comprehensive Handbook*; de Leeuw, K., Bergstram, J., Eds.; Elsevier: Amsterdam, The Netherlands, 2007; pp. 565–592.
20. Shannon, C.E. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
21. Kerckhoffs, A. La Cryptographie Militaire. *J. Sci. Mil.* **1883**, *9*, 5–83.
22. Shannon, C.E. A Mathematical Theory of Communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
23. Albert, A.A. Some Mathematical Aspects of Cryptography. In *A. Adrian Albert: Collected Mathematical Papers*; Block, R.E., Jacobson, N., Osborn, J.M., Saltman, D.J., Zelinsky, D., Eds.; American Mathematical Society: Providence, RI, USA, 1993; pp. 903–920.
24. Friedman, W.F. *Military Cryptanalysis*; War Department, Office of the Chief Signal Officer: Washington, DC, USA, 1938; Volume 1.
25. Friedman, W.F. *Military Cryptanalysis*; War Department, Office of the Chief Signal Officer: Washington, DC, USA, 1938; Volume 2.
26. Friedman, W.F. *Military Cryptanalysis*; War Department, Office of the Chief Signal Officer: Washington, DC, USA, 1939; Volume 3.
27. Friedman, W.F. *Military Cryptanalysis*; War Department, Office of the Chief Signal Officer: Washington, DC, USA, 1941; Volume 4.
28. Friedman, W.F. *Elements of Cryptanalysis*; Aegean Park Press: Laguna Hills, CA, USA, 1976.
29. Konheim, A.G. *Cryptography: A Primer*; John Wiley & Sons: New York, NY, USA, 1981.
30. Schmeh, K. *Versteckte Botschaften. Die Faszinierende Geschichte der Steganografie*; Telepolis-Bücher: Hannover, Germany, 2017.
31. Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*; John Wiley & Sons: New York, NY, USA, 1996.
32. Serra Roig, M. *Verbalia: Juegos de Palabras y Esfuerzos del Ingenio Literario*; Círculo de Lectores: Barcelona, Spain, 2000.
33. García Carmona, J. *Tratado de Criptografía con Aplicación Especial al Ejército*; Ministerio de Defensa: Madrid, Spain, 2011.
34. Yule, G. *El Lenguaje*; Akal: Torrejón de Ardoz, Spain, 2007.
35. Bischoff, B. Übersicht über die Nichtdilpomatischen Geheimschriften des Mittelalters. *Mitteilungen Instituts Österreichische Geschichtsforschung* **1954**, *62*, 1–27. [CrossRef]
36. Mrayati, M.; Alam, Y.M.; at-Tayyan, M.H. *Two Treatises on Cryptanalysis: The Two Essays. The Treatise of ibn Wahab al-Katib*; King Faisal Center for Research and Islamic Studies & King Abdulaziz City for Science and Technology: Damascus, Syria, 2007.

37. Fouché Gaines, H. *Cryptanalysis: A Study of Ciphers and Their Solution*; Dover: New York, NY, USA, 1956.
38. Mrayati, M.; Alam, Y.M.; at-Tayyan, M.H. *Ibn 'Adlan's Treatise, Al-Mu'allaf Lil-Malik Al-'Ašraf*; King Faisal Center for Research and Islamic Studies & King Abdulaziz City for Science and Technology: Damascus, Syria, 2004.
39. Azizi, A.; Azizi, M. Instances of Arabic Cryptography in Morocco. *Cryptologia* **2010**, *35*, 47–57. [CrossRef]
40. Azizi, A.; Azizi, M. Instances of Arabic Cryptography in Morocco II. *Cryptologia* **2013**, *37*, 328–337. [CrossRef]
41. Dávila Muro, J. *Criptología y Seguridad*; Akal, ETSIT, Universidad Politécnica de Madrid-ISDEFE: Madrid, Spain, 2008.
42. Mrayati, M.; Alam, Y.M.; at-Tayyan, M.H. *Ibn Dunaynir's Book, Expositive Chapters on Cryptanalysis*; King Faisal Center for Research and Islamic Studies & King Abdulaziz City for Science and Technology: Damascus, Syria, 2005.
43. Yan, S.Y. *Number Theory for Computing*; Spriner: Berlin, Germany, 2002.
44. Calvo Martínez, J.L.; Sánchez Romero, M.D. *Textos de Magia en Papiros Griegos*; Gredos: Madrid, Spain, 2004.
45. Leary, T.P. Cryptology in the 16th and 17th Centuries. *Cryptologia* **1996**, *20*, 223–242. [CrossRef]
46. Mrayati, M.; Alam, Y.M.; at-Tayyan, M.H. *Al-Kindi's Treatise on Cryptanalysis*; King Faisal Center for Research and Islamic Studies & King Abdulaziz City for Science and Technology: Damascus, Syria, 1987.
47. Kak, S.C. The Vararuchi Cipher. *Cryptologia* **1990**, *14*, 79–82. [CrossRef]
48. Andrew, C. *The Secret World: A History of Intelligence*; Yale University Press: New Haven, CT, USA, 2018.
49. Curatola Petrocchi, M.; De la Puente Luna, J.C. *El Quipu Colonial: Estudios y Materiales*; Fondo Editorial Pontificia Universidad Católica del Perú: Lima, Peru, 2013.
50. Fronczak, M. Atbah-Type Ciphers in the Christian Orient and Numerical Rules in the Construction of Christian Substitution Ciphers. *Cryptologia* **2013**, *37*, 338–344. [CrossRef]
51. Landsverk, O.G. Cryptography in Runic Inscriptions. *Cryptologia* **1984**, *8*, 302–319. [CrossRef]
52. Al-Kadit, I.A. Origins of Cryptology: The Arab Contributions. *Cryptologia* **1992**, *16*, 97–126. [CrossRef]
53. Schwartz, K.A. From Text to Technological Context: Medieval Arabic Cryptology's Relation to Paper, Numbers, and the Post. *Cryptologia* **2014**, *38*, 133–146. [CrossRef]
54. Bingöl, S. Methods for Encryption in Early 19th-Century Ottoman Diplomatic Correspondence. *Cryptologia* **2021**. [CrossRef]
55. Feistel, H. Cryptography and Computer Privacy. *Sci. Am.* **1973**, *228*, 15–23. [CrossRef]
56. National Institute of Standards and Technology (NIST). *Data Encryption Standard (DES). FIPS 46*; NIST: Gaithersburg, MD, USA, 1977.
57. National Institute of Standards and Technology (NIST). *Advanced Encryption Standard (AES). FIPS 197*; NIST: Gaithersburg, MD, USA, 2001.