PLAINTEXT, ENCRYPTION, CIPHERTEXT: A HISTORY OF CRYPTOGRAPHY AND ITS INFLUENCE ON CONTEMPORARY SOCIETY

QUINN DUPONT
PHD DISSERTATION
UNIVERSITY OF TORONTO, FACULTY OF INFORMATION

CHAPTER 1 "REPRESENTATION" – SUBMISSION TO SIGCIS 2015

DRAFT (PLEASE DO NOT DISTRIBUTE)

TABLE OF CONTENTS

Part Three: Ciphertext

PLAINTEXT

In his seminal work on cryptography *De componendis cifris*,[1] Leon Battista Alberti (1404-1472) diverts from his task of exploring and inventing cryptography systems to recall a time strolling through a garden with his friend Dati. In the garden Alberti and Dati got to discussing Alberti's desire to have his cryptography manual printed using the emerging "system of movable type" developed by "the German inventor [Gutenberg]."[2] This convivial introduction to the invention of the polyalphabetic cipher might seem misplaced—after all, the polyalphabetic cipher was a significant invention in its own right,[3] and seemingly unrelated to print and typography. In fact, in Alberti's entire corpus this is the *only* mention of the invention of printing.[4] Yet Alberti notes that it was such discussions with his friend that "brought us to similar appreciations… [of] strange characters with unusual meanings… called ciphers."[5] Rather than being a confused or mistaken association, this leap from movable type to ciphers is intended to signal deeper connections between writing, printing, and cryptography—the way that plaintext is articulated within a notational discourse network that ruptures ancient and medieval notions of representation and resemblances by ushering in ideals of combinatory modularity and indexicality.

Movable type was invented in Alberti's lifetime and proved influential for him; Carpo calls Alberti the first "typographical architect."[6] For Alberti, the invention of movable type highlighted reproducible, modular, indexical, and combinatory logics—logics inherent in the alphabet in the first place, but fully operationalized and made readily apparent in print. Alberti would put these logics to work in both his architectural and cryptographic theory.

Alberti was familiar with the idea of reproducing identical copies from woodcuts, a pre-Gutenberg technique now called xylography.[7] Xylography produced whole "images," typically an etched image or visual depiction. Xylography can even be used to reproduce a complete page (a "single-leaf" woodcut), including textual elements. Entire books—texts and images together—could be printed using xylographic processes, but this "block book" process was rare and may have even originated *after* Gutenberg's invention, as a quick and cheap alternative to movable type.

In either configuration, image or text, producing duplicates from woodcuts was, once the original etching is complete, a comparatively high-speed production technique. However, as Kittler notes, movable type presses were not designed to compete with the speed of xylography, instead they competed with the elegance of manuscript pages.[8] And more to the point, printing from woodcuts, while possible, was relatively uncommon because each successive "edition" introduced the chance of error; this is a critical worry for technical works. The chance of copyist error was so high that authors typically wrote *textual* descriptions of what are fundamentally visual phenomena, such as architectural plans and forms (an "ekphrastic"

[1] *De componendis cifris* was written in 1466 and remained in manuscript form during Alberti's life. A modern English translation by Kim William is available in Williams, March, and Wassell, *The Mathematical Works of Leon Battista Alberti*. References will be made to this edition, using modern page numbers and section divisions. The Latin version has been published in Meister, *Die Geheimschrift Im Dienste Der Päpstlichen Kurie von Ihren Anfängen Bis Zum Ende Des XVI Jahrhunderts*.
[2] Alberti, "De Componendis Cifris," 170 (ii). It seems Alberti was also aware of the work by Arnold Pannartz and Konrad Sweinheim, who introduced Roman typefaces; see March's commentary, ibid., 189. March explains away this passage as an attempt to have his manuscript printed with the support of his patron or perhaps Pope Paul II.
[3] Kahn, *The Codebreakers*.
[4] Carpo, *Architecture in the Age of Printing*, 119.
[5] Alberti, "De Componendis Cifris," 170.
[6] Carpo, *The Alphabet and the Algorithm*.
[7] Carpo, *Architecture in the Age of Printing*.
[8] Kittler, "The Perspective of Print."

mode of expression), rather than employ pictorial techniques so susceptible to copying errors.[9] Alberti was so worried of error that in his architectural works he stressed that copyists should write out numbers in longhand rather than using numeric symbols, even addressing the copyist directly in the work in several cases.[10]

Avoiding the introduction of errors was one of the principle advantages of alphabetic and typographic expression for the reproduction of technical works. Copyists could be counted on to (somewhat) reliably replicate the correct order of a determinate set of icons (the alphabet)—although even here, text rather than numeric symbols was the safer bet. Either way, copyists could not be counted on to replicate intricate pictorial content.[11] To draw a technical image is to invite critical mistakes in the production of new manuscripts or etchings. Carpo summarizes the reticence of those engaged in engineering and scientific communication: "The pretypographical architect knew that for… long-distance transmission, images were not a trustworthy medium. And he practiced his craft within these limitations."[12] Furthermore, the quattrocento era of Alberti is characterized by the expansion of economic, diplomatic, and scientific commerce. Long-distance transmission of materials of many types became vitally important alongside the demands for secret diplomatic communication. To satisfy this need, Alberti argued, cryptography is needed—which has to be secret, capable of long distance transmission, and above all efficient (Alberti calls it "commodious" [*scribetur commodius*]).[13]

Error propagation is a real concern for cryptography. Alberti's polyalphabetic encryption "mixes" multiple alphabets with plaintext that results in a kind of "diffuse" ciphertext. For any one letter of plaintext the corresponding ciphertext may be several letters, or mixed about in unnatural ways. The redundancy of natural languages permits transmission on noisy channels since redundant information accommodates errors. For cryptography, this redundancy is, ideally, deeply compromised. So-called "diffusion" and "confusion" techniques are basic methods available to cryptography, as they frustrate cryptanalytic techniques by "hiding" plaintext more deeply within a combinatory space.[14] The result of highly diffuse ciphertext (what is typically understood as "good" cryptography) is that its transmission becomes very "brittle." Even a small copying or transcription error may render much or all of the resulting ciphertext impossible to decrypt. Very careful transcription, or error-correction codes (as we use today) are a practical necessity for cryptography.[15]

By the fifteenth century the introduction of type begun displacing the process of creating manuscripts by hand, which originally required the inscription of letters *in situ* (at the time of production). On a printed page letters pre-exist as units of type before the creation of words in which they occur. Roy Harris suggests that the "mechanical regularity of print confers upon each alphabetical symbol an independence and a constant visual identity which no earlier form of writing quite achieves."[16] In Alberti's architectural work the letter became a metaphor for modularity, suggesting that the built form can be assembled just like a word created from its constitutive letters.

The invention of the printing press transformed letters from icons in the imagination to manipulatable materials. Individual letters, in the form of literal pieces of metal, were quite obviously distinct from one another, yet each letter produced near-identical impressions with each use. One consequence of this

[9] Carpo, *Architecture in the Age of Printing*, 18.
[10] Ibid., 119. (note 4)
[11] Carpo, *The Alphabet and the Algorithm*, 14.
[12] Carpo, *Architecture in the Age of Printing*, 29.
[13] Alberti, "De Componendis Cifris," 180. (xii).
[14] Shannon, "Communication Theory of Secrecy Systems."
[15] See also Shumaker, who argues that "Copyists—and typesetters—who must toilsomely reproduce long stretches of letters that make no sense to them are peculiarly liable to error; *Renaissance Curiosa*, 100.
[16] Harris, *The Origin of Writing*, 7. For a similar notion, called "decontextualization" see Slaughter, *Universal Languages and Scientific Taxonomy in the Seventeenth Century*.

change was that the letter, not the page, became the locus of identity. Walter Ong suggests that the invention of movable type much more strongly implied a sense of modularity than the written alphabet.[17] The "discrete" letterforms of the printing press were modular and interchangeable, and since written letters had long stood as symbols, the entire system became a modular form of symbol manipulation.

As print suggested that letters are things, letters came to be more strongly indexical.[18] This shift in transitive identity strengthened the link between the sign and the represented thing. Making letters concrete made it easier to see how letters can stand in for more abstract or ethereal things, by moving the mind's eye along with the material icon new combinations and forms of analysis became possible.

According to Carpo, Alberti sought "indexical sameness," and had a "quest for identical replication."[19] Identical replication can also be observed in the identical copies that result from the mechanical print matrix. This explanation, however, admits of some difficulty of interpretation: "indexical sameness" and "identical replication" may not mean the same thing. The printing press (and xylographic processes prior) certainly did create visually identical books—organized pages neatly bound together to create a whole. The creation of identical books was an important and powerful change.[20] This was not the process Alberti capitalized on, rather the invention of moveable type suggested to Alberti ways in which individual letters could be indexical and self-identical.

Alberti's methods for cryptography proposed ways that letters could be self-referential by indexing other letters. With these subtle shifts in identity and reference Alberti opened up a gap between plaintext and natural language. The necessity of type for plaintext forces open the traditional elision between writing and speaking, an elision which Derrida famously labeled "logocentrism."[21]

Derrida argues that metaphysical study searches for an ultimate ground, which naturally leads to what he calls "presence." Western philosophical belief, according to Derrida, privileges the "present," believing it to be that what is most real or true. Ever since the Greek inauguration of philosophical thought, "*logos*" has been a touchstone of presence, a term that means "logic", "reason", "meaning" but also "word." Due to the semantic elision of thought and speech present in *logos* the Greeks prioritized speech over writing. On Derrida's interpretation, Aristotle argued that "spoken words (*ta en te phone*) are the symbols of mental experience (*pathemata tes psyches*) and written words are the symbols of spoken words" (*De Interpretatione* 1, 16a 3).[22] That is, writing is merely a "sign of a sign."[23]

In cryptographic writing the focal point of identity is the individual letter. In *De cifris*, Alberti introduced the basics of encryption by recalling the required substitution of all cryptography: "Thus a common letter, say A, will take on the meaning of another letter, say G…."[24] If Alberti's desire to print *De cifris* had been realized, the transformation from <A> to <G> would have in no way been metaphorical. With movable type an <A> can be literally replaced with a <G>. From the *real* of movable type to the *ideal* of cryptography, the substitution <A> -> <G> is indexical. Each letter's self-identity is required but any visual similarity between <A> and <G> is not needed (in fact, there must be an in-principle way of determining the difference between <A> and <G>). The system works so long as any thing, natural language or otherwise, can be broken down into letters of plaintext, which upon encryption transforms the indexical relationship.

---

[17] Ong, *Orality and Literacy*.
[18] Ibid., 116.
[19] Carpo, *The Alphabet and the Algorithm*, 28.
[20] In many cases, however, printed books remained *sui generis* due to individual differences in production.
[21] Derrida, *Of Grammatology*.
[22] Ibid., 11.
[23] Ibid., 281. In the third chapter we will see how the silence brought about by cryptography severs the logocentric connection between writing and voice.
[24] Alberti, "De Componendis Cifris," 179. "Itaque aut usitate littera uti est .a. aliam quampiam significabit, ut puta .g. et littera .b." in Meister, *Die Geheimschrift Im Dienste Der Päpstlichen Kurie von Ihren Anfängen Bis Zum Ende Des XVI Jahrhunderts*, 134.

In this typographic rupture, philosophized by Derrida, which foretold Alberti's reorientation of indexicality, the exuberance associated with an idealized alphabet would sometimes outpace sensibility. The gap between speech and writing opened by cryptography is actually at risk of inversion, where the letter becomes originary to the voice and fetishized for the visual similarity of printed copies. This inversion is due to the perceived power of letters, which became associated with mystical powers as part of the logomystic tradition. The Aristotelian view that writing is nothing more than a sign of a sign is thus sometimes thoroughly rejected. For example, in a rather vivid way Francis Mercury van Helmont thought that Hebrew letters were a literal homomorphism between the letterform and the speech organs (Figure XX).[25] Over a series of thirty-three woodcuts van Helmont proposed a method of teaching deaf-mutes how to speak by mimicking the shape and movements of the tongue, palate, uvula, and glottis with the shape of Hebrew letters.[26] Eco calls van Helmont's theory "a radical version of the mimological [mimetic] theory," a point we will take up shortly[27] Cryptographers too sometimes drew parallels to esoteric letters. Francis Bacon looked to Chinese in attempting to develop a "Real Character,"[28] Athanasius Kircher looked to Egyptian hieroglyphs (in his *Lingua Aegyptiaca Restituta*),[29] and John Wilkins followed suit, aware of many of these attempts, when it came time to draw links between his description of cryptography and the development of a universal and perfect language system.[30]

Figure XX - *The Alphabet of Nature in which he argued that Hebrew was a proto-language and one that was closest to how the speech organs were intended to be used*

The invention of letters, and then the printing press, also suggested a new combinatory way of thinking. Carpo suggests that the novelty of printing from movable type could have drawn attention to the combinatory logic inherent to the alphabet.[31] For a while combinatorial thinking was even turned into a method—inspired by Ramon Lull (1232-1315), Leibniz called it the "*ars combinatoria*" in his *Dissertatio*.[32] In this early work Leibniz suggested that combining letters and interrogating their resulting configurations, which he called "complexions," could explore all aspects of reality. Each complexion can be organized into a table or run through a mechanism—atomic parts that reveal orders and local relationships.

For all the suggestive implication that the invention of print inspired Alberti's cryptography, *De cifris* remained a manuscript, never to be printed in Alberti's lifetime. Moveable type, while gesturing towards reproducible, modular, indexical, and combinatory logics is not a historical necessity for cryptography. In fact, the *alphabet*, invented some two thousand years prior contained all the analytical logics necessary for Alberti's architectural and cryptographic inventions. Due to the orthographic complexities of some code systems, even, the synthesis of type and manuscript lasted for several centuries past the invention of moveable type, resulting in what Ellison calls "multimodal" production.[33] This is not an issue for Alberti's

[25] As we will see below, the Hebrew (and Chinese and Hieroglyph) alphabet was often singled out for such roles, because it was thought to be relatively pure and free from the corruption brought by the *confusio* after the construction of the tower of Babel.
[26] Eco, *The Search for the Perfect Language*.
[27] Ibid., 83.
[28] Bacon, *The Two Bookes of Sr. Francis Bacon. Of the Proficience and Aduancement of Learning, Divine and Hvmane*; Bacon, *Of the Advancement and Proficiencie of Learning*.
[29] Stolzenberg, *The Great Art of Knowing*.
[30] Wilkins, *Mercury: Or the Secret and Swift Messenger*.
[31] Carpo, *Architecture in the Age of Printing*, 54.
[32] Leibniz, *Dissertatio de Arte Combinatoria*. An English translation is available in Leibniz, "Dissertation on the Art of Combinations."
[33] Ellison, "Millions of Millions of Distinct Orders."

manuscript, nor many printed schemes such as Francis Bacon's bi-literal cipher (in his *De Augmentis Scientarum*).[34] John Wilkins' complex scheme for a perfect language and a cipher in *Mercury*, however, would require manual additions to the typescript, since Wilkins' notation outstripped the capabilities of reproduction technologies of the time.

Alberti's notation

Alberti stood at the crossroads of the development of a notational discourse network. The structure of his discourse as well as his methods are those of the medieval Scholastic tradition, so full of visual realism and resemblance, and yet, for example, in his *De re aedificatoria* he manages to formalize ancient architecture without illustrating or even describing it. In Carpo's assessment Alberti's architectural theory "cleanses itself" of the practice of imitation, or "mimesis."[35] Even though Alberti was an accomplished and famous theorist of painting—the very prototype of mimetic representation—in his architectural works there seem to have been no drawings of ancient monuments, and not even ekphrastic reconstructions of any buildings.

In place of mimetic representation Alberti utilizes a "notational" form of representation in his development of multiple writing machines. In *Descriptio Urbis Romae* (Figure XX), Alberti develops an ingenious device to plot the coordinates for a plan of Rome. Avoiding the issues involved in scientific and engineering communication using mimetic, visual descriptions, and the errors these methods potentially introduce, Alberti's "reconstruction of Rome" lists the coordinates of points, plotted with the ruler pinned to the center of the circular horizon. By matching notations on the ruler to notations along the circumference of the horizon the user can recreate the plan of Rome by first plotting points and then, in a kind of connect-the-dots way, draw the outline of the plan. Carpo rightly calls Alberti's invention a way of producing "digital images."[36] When his plotting machine (hardware) is combined with the appropriate method (software) and fed suitable coordinates (data) it produces images. Alberti even expands the scope of the mechanism in *De statua* for use in three dimensions as a way to re-present the human body.[37]

Figure X: *Descriptio Urbis Romae*

There are interesting and significant parallels between Alberti's mechanism for architectural plans in *Descriptio* and his cryptographic invention in *De Cifris*. *De Cifris* culminates with a method and mechanism for polyalphabetic encryption using a cipher wheel. The cipher wheel Alberti describes is composed of two rotating, circular planes that are attached to a center pin upon which they rotate around (Figure XX). Along the circumference of each plane is written an alphabet. The cryptographic "key" is set by aligning two letters, viz. "say such k lies under the upper-case B."[38] Substituting each letter of the plaintext to its "twin" along the other plane encrypts the message. Used as such, Alberti's cipher wheel is merely a handy mechanism for common substitution ciphers (known since antiquity as a "Caesar" cipher, although its providence is likely much older). Alberti's cryptographic innovation is his addition of multiple alphabets—he writes, "after I have written three or four words I will mutate the position of the index in our formula, rotating the disk let's say, so that the index k falls below the upper-case R."[39] By rotating

[34] Bacon, "Translation of the 'De Augmentis,'" 108 ff.
[35] Carpo, *Architecture in the Age of Printing*, 120.
[36] Ibid., 123.
[37] Ibid., 122. Carpo notes that "the key piece of hardware in Alberti's *De statua* was a revolving instrument, a wheel of sorts, in this case somehow inconveniently nailed to the head of the body to be scanned" Carpo, *The Alphabet and the Algorithm*, 55.
[38] Alberti, "De Componendis Cifris," 181. (xiv)
[39] Ibid.

the disk during the process of encryption a "new" alphabet is introduced each time, making cryptanalysis significantly more difficult and increasing the combinatory space.

Figure XX: De Cifris

The cipher wheel works "digitally" just like the architectural device in the *Descriptio*. To be more precise, we can say that Alberti's cipher wheel capitalizes on the way that words can be decomposed into modular, discrete things. Natural languages have particular identity requirements and redundancies—most noticeably visible in word and letter divisions. Each language, and each form of expression, brings about its own syntactical characteristics, which can be imperfectly remediated and translated only with the greatest of difficulty. For natural languages "translation" is necessarily a failure.[40] Alberti's cipher works on the level of what he calls "natural" syntaxes; he relates the intrinsic qualities[41] of Latin letter "orders" to "numeric ratios,"[42] as vowels and consonants, bigrams and trigrams.[43]

These natural identities are first "scrambled" about, but like a dutiful caretaker collecting leaves blowing in the wind, cryptography then rakes the leaves into piles, forcing artificial identities and orders.[44] The technique Alberti invents with his cipher wheel places individual letters into "houses;"[45] the smaller wheel of the cipher contains "mobile" houses. Together, the two wheels are a formula,[46] where the relative positions of the houses (the "index") are like a "key." The process is only possible with the totality of the system, that is, encryption and decryption can only occur if the parts of language have been stored in the houses and their relative positions adjusted and remembered.

In hindsight the architectural and cryptographic machines Alberti produces in the *Descriptio* and *De cifris* invite comparisons to modern computers. Thus, Alberti's mechanisms were in many ways too far ahead of their time. A theory of technical communication necessary to explain the functioning of Alberti's machines would not developed until the twentieth century, and furthermore a description of the notational discourse network Alberti stood at the crossroads of is, even today, still wanting.

With his radical technique Alberti's work can be seen as railing against ancient theories of representation, communication, and media. In stark opposition to the prevailing theories of handcrafted representation (painting, sculpture, and so on), Alberti's work ushered in a method for mass production; mass production of built form and mass production of expression.[47] Just as Alberti's architectural methods gave rise to "designed" buildings—in distinction to the old handicraft of architecture previously—his cryptographic methods ushered in an implicit separation of the existing elision between speech and things by self-referentially indexing letter to letter.

Alberti was a champion of a new kind of "indexical" sameness, but not the sameness of mass production where every piece is identical, as though stamped out from a form or mold. Carpo notes that in Alberti's world of handicraft, "imitation and visual similarity were the norm, replication and visual identicality were the exception."[48] Alberti's methods were powerful because they offered identicality when desired, but also permitted modular adjustment and reordering. The building blocks of printed letters provided the model from which Alberti developed his notational architecture and cryptography.

---

[40] This is the subject of Chapter 7.
[41] "*De notis literarris quales sese natura*" (iv).
[42] "*numeri rationibus*" (iv).
[43] See Alberti, "De Componendis Cifris," 173–178.
[44] Ibid., 179 (xi). Della Porta also discusses the "dislocations of the natural order of letters," see Shumaker, *Renaissance Curiosa*, 116.
[45] "*hae partes domicilia nuncupantur*" (xii).
[46] "*formulam*"
[47] C.f. Carpo, *The Alphabet and the Algorithm*.
[48] Ibid., 3.

Alberti's advances towards a notational form of architecture would, in fact, eventually be rolled back. The introduction of powerful computers in the twentieth century, working directly with an inner (binary) notation, would end up being used for visual design—an ancient, mimetic, even "painterly" form of expression. Today, CAD programs are thoroughly mimetic, and it is only at the fringe of artistic practices that algorithms are used *directly*, countenancing Alberti's methods. Alberti's cryptographic work fared somewhat better—his theory and mechanism would prove popular (if invisible), but it too had to draw on novel, sometimes unusual traditions to crawl out from under the heavy weight of a pervasive and powerful mimetic theory.

Starting with Plato and Aristotle, mimesis would prove to be the most powerful and popular theory of representation, an endowment that it probably still holds today. This power meant that all forms of communication were understood as examples of mimetic prototypes, examples of art rather than technical media.

Mimesis and media

Mimesis is the traditional theory of mediation. But mimesis was never intended to describe the processes and stuff that we call media, that form of communication—usually technical—which properly dominates modern life. Since its inception in antiquity mimesis was, and still is, a theory of art and aesthetics that investigates *poiesis*, or "making." Mimesis describes the way humans make representational objects, but not the way that these objects stand "between" subject and object. Instead, mimesis posits a duplication of the represented object. This duplication ends up being cashed out in terms of subjective realism.

As we will see, any theory of subjective realism—even a very subtle one—is a poor theory of representation for understanding the functioning of plaintext. Such theories of mimesis perform ably for many domains of representation, from painting to creative writing, but over the last millennium certain kinds of technical making have proven extremely successful and, in retrospect, end up looking rather different from those that came before. Most generally, this special kind of technical making I am referring to is the production and operation of "code," for which plaintext is a subset. There is a important potential broader project here—coming up with a theory of representation subtle and deep enough to describe and illuminate the representational qualities of code and its long development, but this is not to be attempted here. Although it is recognized that the mimetic theory needs to be rejected (or at least radically altered,) to explain code, my goal is only to offer a short genealogical account of mimesis (through some of its various incarnations), and then to describe the representational parameters of an alternative. The alternative I propose is a theory of "notation," which I do suspect underpins much if not all contemporary workings of code, but for my purposes the theory of notation is strictly-speaking only with reference to plaintext.

Media often function without code, but so-called "new" media typically gains (representational, social, political, psychological) power through code. There are, however, much older forms of media that function through code—cryptography being the obvious case. Despite these ancient historical antecedents, describing how code mediates is challenging work that has only very recently been taken on as an academic project. Without doubt the newness of the materials makes such analyses complex and incomplete; there is another explanation as to why it is so very difficult to explain how code mediates, and why we have only very recently taken up the challenge. This reason is a historical quirk—Aristotle founded the study of technical media in his psychological work—and proved the intellectual success and analytical power of the theory of mimesis.

Until recently there had been no theory of media in the way that we understand the term. In fact, John Guillory reports that the very concept of media, "was absent but wanted for" the several centuries prior to its eventual appearance in the twentieth century.[49] Guillory looks to Aristotle's *Poetics* for a media theory and returns wanting. Guillory investigates the *Poetics* because Aristotle tackles the question of a "medium"

[49] Guillory, "Genesis of the Media Concept," 321.

but quickly sets it aside, where "it remained for two millennia."[50] Kittler also pins the blame on Aristotle.[51] He argues that Aristotle's very concept of ontology is incompatible with the concept of technical media since it describes things in their matter and form, but not the relations between them. Seeking to find a theory of mediation capable of explaining technical media, Galloway offers the counterpoint, that Kittler was in error when he said the Greeks had "no theory of mediation."[52] The Greeks, Galloway points out, believed that the Muses mediated many things: Aphrodite was "middle-loving," Hermes transmitted messages, and Iris mediated between immanent things.[53] But, despite Galloway's revisionist history, the actions of the Muses (and later, angels) went unacknowledged as legitimate forms of mediation. The concept of a physical medium acting "between," as Aristotle set it out, was relegated to a theory of sensorial perception where it seems to have languished.

Ancient theories of mimesis

The invention of writing must have been a protracted yet marked disruption to the social fabric of its time, perhaps much like the development of computers today. But because we live in a literate world, we naturally accept the way that the written word mediates communication and thus rarely see the specular effects it produces. According to the ancients, still very much grappling with the relatively new (and developing) media technology, writing duplicated the world. Writing was, perhaps naturally, grouped together with other arts, producing profound changes to how we think and communicate. There are, of course, many ways this change could be have understood, but for the ancients writing duplicated speech in particular. Speech was seen as more natural, and more "present" (recall Derrida's critique, described above). This process of duplication was given the name "mimesis."

The alphabet was invented around 1500BCE by Semitic people around the same location that the first script was invented some 2000 years prior (around 3500BCE). Conceptually, although not necessarily practically, the invention of the alphabet created a new form of expression that cut ties with the pictorial representation inherent in all previous forms of script.[54] The remarkable fact is that while there have been many scripts,[55] there is only one alphabet; all alphabets originate from the Semitic invention.[56] The Semitic alphabet was then adapted by the Greeks to develop, for the first time ever, vowel letters. In previous non-vowelized alphabets, as we still see in the alphabet of modern Arabic, diacritical marks were used to indicate vowels sounds where the reader could not supply them on her own. This shift, according to Ong (following Havelock) and Kittler, was profound. By marking vowel sounds the Greek alphabet was able to represent phonemes (thought to be the building blocks of spoken language), which made writing easy to learn, and provided a capacity for expressing foreign languages and thoughts.[57] For this reason Ong calls the Greek alphabet "democratic" and "internationalizing."[58]

---

[50] Ibid., 323.
[51] Kittler, "Towards an Ontology of Media."
[52] Galloway, *The Interface Effect*, 15.
[53] This is the subject of Chaper 6.
[54] The most pictorial of the scriptural forms was the pictograph. Other pictorial scripts were invented too, such as ideographs like Chinese script which symbolize pictorially but does not necessary directly relate to the represented *word*. For example, in Chinese script a picture of a tree represents a tree, but two trees represent the distinct concept of "woods". In ideographs there are no direct relationships between phonemes and the pictorial content. See Ong, *Orality and Literacy*, 86.
[55] A script is distinct from the many ways that early humans used external memory aids, such as tally sticks, pebbles, and "winter count" calendars. Ong describes a script in the "sense of true writing" as consisting not of mere pictures or representations, but of "a representation of an utterance, of words that someone says or is imagined to say." Pictorial expressions, such as hieroglyphs, therefore count as scripts. See ibid., 83.
[56] Ibid., 85.
[57] Ong, *Orality and Literacy*; Kittler, "The History of Communication Media."
[58] Ong, *Orality and Literacy*, 89.

Before the invention of writing was fully interiorized, the Greek playwright Homer lived in a world that was fundamentally oral. Human expression in oral cultures differs significantly from those in literate ones. Almost a century ago Milman Parry claimed that virtually every distinctive feature of Homeric poetry is due to its oral mode of composition.[59] The strange, formulaic feel of Homer's work is due to it being "stitched together" from standardized expressions (the Greek term "rhapsodize" means "to stitch song together").[60] Because of its oral mode of composition, Homer's work reflects an inherent mnemonic structure—without writing, strategies for memory had to be an internal part of the expression. Thus Homeric expression is rhythmic, repetitive, additive, redundant, and so on.[61]

By Plato's day, the Greeks had effectively interiorized writing. Plato's famous dismissal of writing, which was *written* in the *Phaedrus,* argued that the introduction of writing would cause the loss of memory. In the *Republic,* Plato argues against the (typically oral) poets, suggesting that they should be cast out of the perfect city. Plato's argument against the poets hinged on an elaborate argument against the duplication of reality, especially duplication based on falsehood and immoral or unjust beliefs. This process of duplication and imitation extends from the oral poets and their mythic speech (such as in Homer) to other imitative art forms—painting, sculpture, and writing.

The process that unifies the range of different kinds of human expression was given the name "mimesis." Plato, and later Aristotle, would develop a theory of mimesis that would persist, with occasional alteration, to the present day. One of the consequences of such a complex and powerful theory of human expression is that it has the potential to obfuscate differences among distinct kinds of expression. For our purposes, it is significant that notational writing is lumped in with the rest, as though plaintext was just another form of expression like speech or sculpture.

Prior to Plato's *Republic*, the Greek term "mimesis" had a non-philosophical, mundane sense of—roughly—the act of miming or a person who mimes. We know about this sense of mimesis from maybe five pre-Platonic sources.[62] The Homeric epics, which would later figure prominently in Plato's critique, describe mimesis as the retelling of narrative in a dichotomy between truth and falsehood—a kind of doubling between poles of opposition. In a fragment by Gorgias, this dichotomy is extended from truth and falsehood to an antithesis of pleasure and instruction. Gorgias, like Plato would later argue, believed that mimetic poetry is a form of deception that works by "magic and allurement." Xenophon thought that there was a formal correspondence between the subject and object of mimetic art at the level of ordinary visual phenomena (a view that is sometimes still unreflectively offered). And finally, in Aristophanes' *Frogs*, a positive view of mimetic art is offered. Aristophanes saw the poet as a creative "maker" who stood on the same footing as other craftsmen.

Plato's theory of mimesis

Plato developed this existing sense of mimesis into a sustained philosophical position. Plato's critique focused on how mimetic arts merely "imitate" the deeper reality he posited in his theory of Forms. In this way Plato was a kind of objectivist: mimetic art should be judged by its ability to represent the external and objective standards of (ideal) reality. The two primary locations for Plato's discussion of mimesis are his *Ion* and *Republic*, to which we will now turn.[63]

In the *Ion*, Socrates forces the eponymous rhapsode Ion to admit that the only poet he is only capable of speaking about is Homer. Socrates suggests that Ion's inability to speak about other poets is because rather than using mastery (*techné*) of a general body of knowledge about poetry, he is "possessed" or "inspired" from the Muses. The idea that "inspiration" is the source for poetry is extended to include other

[59] We know of Homer's work only because after being composed orally, and repeated in memory, it was written down many years later.
[60] Ong, *Orality and Literacy*, 22.
[61] Ong offers an extensive list of the psychodynamics of expression in an oral culture; see ibid., 36 ff.
[62] See Halliwell, *Aristotle's Poetics*.
[63] English translations from Plato, *Complete Works*.

forms of art, such as sculpture, singing, or instrument-playing. In fact, Socrates argues, even Homer himself does not draw upon a body of knowledge but is also inspired by the Muses.

Socrates argues that truly inspired art cannot be created when of the "right mind." Just as we might say of artists today, Socrates argues that great art is a "divine gift" in which over-thinking inhibits the process. God, Socrates claims, takes the poets' "intellect away from them when he uses them as his servants."[64] This emptying of knowledge has an important consequence for Plato: art does not proceed by way of truth, but is instead a madness or irrationality. In what will turn out to be a central difference with Aristotle, Plato aligns techné (or "making") with the irrational, inspired source of mimetic art.

Socrates then makes an allusion to iron rings connected by a magnet.[65] The central magnet attracts the iron rings because it puts its power into the rings, which in turn put their power into other rings, and so on, until the magnetism is finally used up. On the allusion, Homer is the first, most divine ring, having received his poetic gift directly from the Muses; Ion is a more distant, lesser ring, who does not possess the same divination as Homer. Homer is a representative of the divine, but Ion's recitations are even worse: he is a mere representative of a representative (doubly imitative). Each more distant ring from the original inspiration is a further derivation (and depletion) of whatever reality and truth the original might have possessed.

In Plato's early work *Ion*, the arts are seen as derivative and tenuous. But, the term "mimesis" is never used, and thus we don't have a full sense of "imitation." By the *Republic*, however, Plato explicitly uses the term "mimesis" to describe the arts.

In Book III of *Republic*, Socrates and Adeimantus discuss the ideal composition of their proposed state. While reciting the poetry of Homer, Socrates argues that in an ideal state poetry will be excluded in both content and form. Certain messages must be restricted because they are liable to be imitated by the youth and thus bring about negative effects. The messages must be restricted, but Socrates goes further still and argues that the "style" or "how it should be said" must also be restricted.[66] Socrates now formally introduces mimesis, as a kind of performance or "story-telling."[67] Like in *Ion*, the imitative effect requires that the poet "hides himself,"[68] and the concern is again the lack of mastery of skill, or failing to "achieve distinction."[69] As is typical of Plato's characterization, he sees the mimetic arts as enactive and performative, but it is also clear that he does not require this narrow characterization of performance for mimetic art. Rather, Plato tends to waffle between the performative and formal qualities of mimesis; Plato's position can be compared with Aristotle, who, for example, believes that mimesis is "possible without a public performance and actors."[70] Plato tends to characterize mimesis as literal imitation rather than more complex forms of realism, verisimilitude, or representation.

In the *Republic*, Plato extends the predominantly aesthetic approach found in *Ion* to morality and politics: by setting up a derivative, false reality, imitation of this world is the cause of slavish or shameful actions.[71] The mimetic effect is also extended into psychology and social relationships. Plato's concern stems from the irrationality of the origins of mimesis, and its potential to cause behavioural imitation (especially in the youth). Together, this cause and effect make mimesis like a drug: it is powerful and useful when administered correctly, but dangerous when used improperly.

In Book X, Plato continues his discussion of how the origins of mimesis are irrational and illusory, and that its powerful imitative effect leads to troublesome personal and social behaviour. In a discussion with Plato's brother, Glaucon, Socrates extends the earlier prohibition of poetry to all imitative arts. Using an

[64] *Ion*, 532c.
[65] *Ion*, 533d.
[66] *Republic*, 392c.
[67] *Republic*, 394c.
[68] *Republic*, 393d.
[69] *Republic*, 394d.
[70] *Poetics*, 1450b15.
[71] *Republic*, 395c.

implied argument about god established earlier in the *Republic*, Socrates argues that there are three levels of reality,[72] exemplified by the makers of a couch: first there is the idea of a couch, made by god—the "natural maker"—which is necessarily singular; second are material couches made by craftsmen who strive to be like god, imitating the original Form but who do not "truly make [*poiesis*] the things themselves;"[73] and third are the imitative arts, such as painters, who do not imitate the original but simply imitate the (imitated) material works of craftsmen. To show how false and illusory both the craftsman and the painter are, Socrates imagines a "clever and wonderful fellow" who walks around with a mirror and claims to be "making" all the things of the world as he points it towards objects.[74] This fellow with the mirror, obviously, is only fabricating the "appearance" of things.

The metaphor of the mirror pertains to visual mimesis, but it should be understood as analogous to other non-visual forms of mimesis too. As discussed in *Republic* III, mimesis applies to poetry as well as visual arts. The key to poetry, for both Plato and Aristotle, is *muthos*, which originally meant simply "content" but in Plato's hands took on the sense of distorting "myth." Plato often aligns the mimetic qualities of the performance of poetry to formal qualities of visual arts (colours and shapes). However, the *muthos* of language—poetry, epic, tragedy, and so on—is also part of mimesis, as Aristotle would further develop.

In Book X we see a serious ontological and epistemological challenge stemming from mimesis. Like the famous "allegory of the cave" discussed earlier in the *Republic*, a complete shift in ontological thinking has occurred: truth is no longer to be found in the material things of the world (neither the material couch nor the painting of it), but instead resides in the intellect alone. While maintaining a critique of imitative art, the world that we know and experience is also a mere imitation in Plato's hands.

Aristotle's theory of mimesis

Aristotle's views of mimesis are for the most part found in his *Poetics*. In this work, Aristotle describes detailed criteria for differentiating between the forms of art; the source of mimetic arts, as rational and structured; and the result of mimetic arts as either education, ethics, or pleasure. These criteria and descriptions hinge on Aristotle's analysis of *techné* and *poiesis* and the bulk of the *Poetics* is devoted to differentiating between forms of mimetic art. Aristotle differentiates between poetry (with a fragmented/missing section on comedy), tragedy, and epic, while also contrasting visual arts throughout (such as painting and sculpture). The formal qualities of each type of art are dictated by mimesis, and can be used as natural demarcations.

According to Aristotle, there are two natural, human causes of poetry: from childhood we are naturally imitative, and we take pleasure in works of imitation.[75] Further, poetry can be analyzed by "differences in character" within narratives.[76] For example, tragedy, distinct from poetry, is an imitation of a "serious" action that is "complete in itself" (in the sense of being rational and structured).[77] Tragedy can also be pleasurable despite its "serious" topic—even when the topic is "painful to see."[78] While the pleasure from tragedy is unique and offers different opportunities for education, it is however, simply a species of a more general pleasure from mimetic art.

A central concern for Aristotle's *Poetics* is *muthos*, which took on a pejorative valence for Plato, but is significantly reimagined in the *Poetics*. Halliwell translates *muthos* as "plot-structure," which is not simply the abstract shape of the plot, but the totality of the represented action with all its causal connections and development.[79] Aristotle argues that *muthos* is not simply mimetic actions strung together into a narrative,

[72] *Republic*, 597ff.
[73] *Republic*, 596e.
[74] *Republic*, 596d.
[75] *Poetics*, 1448b5.
[76] *Poetics*, 1448b25.
[77] *Poetics*, 1449b20.
[78] *Poetics*, 1448b10.
[79] Halliwell, *Aristotle's Poetics*.

rather, the structure must be "complete in itself, as a whole of some magnitude."[80] This "whole" must have a beginning, middle and end that are "naturally" connected. It is the *muthos* structure that creates a feeling of completion, direction, and justifiable connection within a plot (versus a plot that lacks compelling features, zigging and zagging without reason). According to Aristotle, good plot-structure is created by mimesis' connection to reason, not inspiration or madness as Plato argued.

Aristotle argues that mimetic arts can result in beneficial education, helpful alignment to moral issues, and even pleasure. The educational value of mimetic art is closely associated with its ability to provide pleasure to its audience. In part, Aristotle argues, learning is itself "the greatest of pleasures."[81] Furthermore, mimetic art can "gather the meaning of things" directing one's gaze from particulars to universals.[82] Even in the case of mimetic arts that are fictional or truly novel—such that the viewer does not have an existing referent for the mimetic subject—these too can be educational and pleasurable. For fictional and novel mimesis Aristotle claims that the educational and pleasurable value does not simply lie in the formal qualities of the mimetic art—"the execution or colouring or some similar cause"—but rather in the rational structure of the representation itself.[83]

Whereas Plato was unable to disassociate the moral and aesthetic qualities of mimetic art, Aristotle developed a theory of mimesis that can (but does not only) judge aesthetic qualities on their own terms. However, like Plato, Aristotle argued that aesthetics should be conformable to moral and political principles, and still consistent with reality (especially reality perceived through universals). For example, a horse drawn correctly but with poor talent is not as good as a horse drawn with only a technical error (e.g., legs facing the wrong way) but which does not fail "in the essentials of the poetic art."[84] Similarly, it is better to portray good men (or, "as they ought to be"), but precedence should be given to how artistically the activity is conducted.

Mimesis is an important way of understanding how a great deal of human expression works, and we still live in the shadows of ancient theories of mimesis. While sophisticated and various in their approaches—Plato opposing mimesis in favour of his own ontological approach, Aristotle seeing considerable value in mimetic arts—ancient views of representation were still fundamentally configured around the illusions and realisms of mimesis.

Late Medieval and Renaissance web of resemblances

To carry forward the ancient theories of mimesis—up to their historical breaking point—we must turn to the late Medieval and Renaissance theories of representation. This was an enormously intellectually rich time, as the West was throwing off the shackles of what was perceived to be a previous "dark" ages (at least according to the Humanists), the accumulation of considerable material wealth in trade cities, new science and technology, and the flux of three Abrahamic faiths. During this time the narrative of mimesis loosens its grip and starts to relinquish its relation with knowledge, if only a little. Representation was still posited as a form of repetition, a theory of language which pictured the "universe… folded in upon itself," as Foucault describes it.[85] During this period the Greek term and the philosophical concept of mimesis fades, but only to be replaced with an extremely rich semantic web of resemblances. Foucault identifies ten such notions, gathered from the jurist (and follower of Ramon Lull, whom we will encounter shortly) Pierre Grégoire's *Syntaxeon artis mirabilis.* Of these ten, Foucault states that four are essential to understanding resemblances at the end of the sixteenth century. It is with Foucault's list of "essential" notions of resemblance to which we will start.

---

[80] Ibid., 5.
[81] *Poetics*, 1448b10.
[82] *Poetics*, 1448b15.
[83] *Poetics*, 1448b20.
[84] *Poetics*, 1460b20.
[85] Foucault, *The Order of Things: An Archaeology of the Human Sciences*.

Convenientia in memory technologies from Lull to Alberti's cipher wheel

The first notion is *convenientia*, which denotes "adjacency of places." Foucault describes the sense of "convenience" as those things which come sufficiently close to one another; a resemblance appears within the hinge of convenient things.[86] Adjacency in nature is not an exterior relation in this world, but rather a (perhaps obscure) sign of a relationship between things. In the vast syntax of the world, the relations between things have hidden reasons for their propinquity.

To understand how *convenientia* operates on appearances, and to see why and how a scientific method might arise in this web of resemblances, we need to turn to an unlikely tradition, the art of memory as developed through antiquity. Of the three most famous mnenotechnical works in antiquity, Quintilian provides the clearest picture of the method.[87] To fix items firmly in the memory, he states, one must place the items to be remembered within an architectural scene (called "*loci*"), either associated with houses along well-known street, or in later incarnations, a room with nooks for mental placement (recall Alberti's description of the indexes of his cipher wheel, described as "houses"). To recall the items from memory the person simply has to move from one space to the next in the mind's eye. The basic method can be further refined (and over the years there were many adaptations): each fifth item can be given a distinguishing mark, the memory spaces should be made very distinct and not too crowded, it may be useful to employ memory for "words" instead of "things", and (as was particularly common in the middle ages) the use of arousing images may help cement items within the space.

Unlike most ideas from antiquity, knowledge of the art of memory did not depend on transmission through the Christian Fathers or the (later) Arabic translators. The art of memory was known, it seems, directly through the lively rhetorical tradition (specifically through the *Ad Herennium*).[88] Throughout the middle ages, however, the art of memory changes its originally stated purpose as outlined in the ancient sources. Since the rhetorical tradition was being sustained by religious orders during the middle ages, the art of memory came to be used for remembering pious things, and as a mechanism to assist natural devotion (not unlike how prayer beads are used today). With new religious associations the art of memory took on an ethical importance.

By the thirteenth century, Thomas Aquinas changed the method of the art of memory, retaining *convenientia* but replacing the ancient use of architecture for memory places with a method based on "corporeal similitudes."[89] These are startling changes, since the adapted technique was given religious importance, only to be converted to use corporeal or even profane imagery. Thomas argues that this adaptation is necessary because "it is natural for man to reach the *intelligibia* through the *sensibilia* because all our knowledge has its beginning in sense."[90] Thomas' development shifted how representation works, from a rather mechanical method of memory to an epistemic investigation.

Thomas' method would enter into the Renaissance's own complex web of resemblances. On the one hand "corporeal similitudes" would continue to be used and adapted, especially as hermetic imagery became popular. On the other hand, a revival of the ancient architectural (non-pictorial) method also occurred, including the development of specifically designed (real or imaginary) rooms that offered good memory locations.

As we move forward in time it might be expected that the influence of memory arts would wane, after all, it was recognized that the printed book ought to destroy memory (as Plato complained about writing in antiquity). Furthermore, during the Renaissance more careful study of the ancient techniques of memory (with the re-introduction of Quintilian's clear exposition of the art) helped to expose the medieval "perversion" of adding similitudes to the otherwise non-imagistic method (Humanist authors, such as

[86] Ibid., 21.
[87] Yates, *The Art of Memory*.
[88] Ibid.
[89] Ibid., 76.
[90] *Summa Theologia*, I, I, qI, aXVIII.

Erasmus were particularly opposed to these kinds of medieval additions). But, Yates argues, the memory arts received a new lease on life with the revived neoplatonic movement inaugurated by Marsilio Ficino (1433-1499) and Pico della Mirandola (1463-1494).[91]

The body of writing known as the *Corpus Hermeticum* was rediscovered in the fifteenth century and translated into Latin by Ficino. The *Corpus Hermeticum* was believed to be of ancient Egyptian providence, written by one Hermes (or Mercurius) Trismegistus. Through Ficino's Latin translation and his considerable influence, Giulio Camillo (ca. 1480-1544) created a memory "theatre" making extensive use of the hermetic parallels of microcosm and macrocosm. By interpreting hermetic doctrine Camillo designed his memory theatre to reflect humankind's place within the universe. The theatre was not just efficacious because it made use of the practical *loci* method of memory inherited from antiquity, rather the *loci* of the theatre were a microcosm of the universe— arranged, numbered, and named all in accordance with a reflected reality. Impressive feats of memory were possible because the theatre let humankind tap into a divine memory. Similarly, Pico adopted the divine measures of the celestial world from cabalism. The divine names were also adapted from cabalism by Camillo for use in his theatre. Yates describes the synthesis of hermeticism, cabalism and memory arts as follows:

> *In this world, man with his mind made in the image of God has the middle place.… He can move amidst it with understanding and draw it into himself with subtle religious magics, Hermetic and Cabalist, which bring him back on to that divine grade which is his by right.*[92]

So far we have seen how *convenientia* operated within the web of resemblances up to the Renaissance. From its ancient roots in rhetoric it was employed as an art of memory that functioned quite distinctly from our previous discussion of mimesis, but as the memory arts developed through the middle ages these resemblances lost some of their purely "convenient" character of adjacency and picked up a more imagistic, mimetic utility. By the Renaissance, mimetic resemblances had accreted new neoplatonic properties that took the images of the memory arts further into the depths of reality, posited as a reflection of an emanative first principle.

Convenientia has a second tradition not yet discussed, the *Ars* (or Art) of Catalan thinker Ramon Lull (1232-1315). Lull unifies the loose ends we have seen so far, the shifting web of resemblances from the ancient rhetorical tradition, the re-introduction of mimetic images into an art of memory that took on ethical and religious importance, and (discussed below) Bacon and Vigenère's cryptanalytic method of interpretation. The unification of resemblances came under one Godhead, an art that mirrored the Christian Trinity: *intellectus*, an art of knowing and finding Truth; *voluntus*, an art of training the will towards loving Truth; *memoria*, an art of memory for remembering Truth.

Lull's art differs in many ways from the classical version we have seen so far.[93] First, Lull's art does not originate from the rhetorical tradition, rather it comes from an Augustinian Platonism with elements of popular neoplatonism. Lull's method, which later influenced philosophical language planners (discussed below), claimed to articulate, and to start from, first causes—what Lull called "*Dignitates Dei.*" This is in sharp contrast to the rhetorical tradition, which sought to duplicate the world and gain access to it through a series of similitudes and images; Second, drawing from some distant Platonic traditions in opposition to the use of mimetic representations Lull opposed the medieval use of images used to excite the memory. In place of these mimetic images Lull used only (primarily alphabetic) notations to hold items in the memory and to investigate reality. Third, Lull adds movement to an otherwise static classical tradition of memory, were the memory items are in place as static *loci*. Lull's method used rotating wheels that made the old medieval encyclopedic schemes seem rigid.

Nearly two centuries later Lull's tripartite mechanism developed into Alberti's cipher wheel. Kahn reports that scholars typically assumed Alberti's cipher wheel was inspired by his architectural "horizon"

---

[91] Yates, *The Art of Memory*.
[92] Ibid., 150.
[93] Ibid., 175 ff. A translation of some of Lull's work, including the *Ars Brevis*, is available in Llull, *Doctor Illuminatus*.

(probably the *Descriptio Urbis Romae* described previously), the astrolabe-type device used for surveying.[94] Kahn argues that this is an unconvincing source because while both devices are circular and divided into sections, the critical idea that marks are juxtaposed and read together is missing in the horizon device. Instead, Kahn suggests that Alberti's cipher wheel was directly inspired by Lull's rotating wheel (or "volvelle").

In Lull's *Ars Brevis*[95] the first "figure" arranges the divine "dignities" into two circles, with each slice designated by a mark rotating against each other (Figure XX). The outer ring of nine letters (B, C, D, E, F, G, H, I, K) aligns against the inner ring of dignities, arranged in *convenientia* (in the first figure, which is denoted by "A", the dignities are "goodness, greatness, eternity" and so on).[96] The disks rotate to create new prepositions, such as "goodness is great" and "greatness is good."[97] With each rotation new associations are explored. Lull also notes that "because each letter can have many meanings, the intellect becomes more general" and abstract, akin to the way that the mind moves from the particular to general in Aristotle's view of scientific investigation. The intellect climbs a "ladder" as combinations are understood.[98] The method, along with "the alphabet" and their signifieds must be "learned by heart."[99] Each letter also works like the *loci* of the memory arts, holding in the mind a particular notion for consideration. Considered in its tripartite structure, with each turn of the wheel the will is activated, the intellect considers the combination, and the memory attempts to fix the preposition in its *loci*.

Figure XX: Figure A, *Ars Brevis*

Alberti's cipher wheel (Figure XX) bears a striking resemblance to Lull's first figure.[100] On Alberti's design each disk is divided "into twenty-four coequal parts; these parts of the circle are called houses."[101] The division into "houses" is also strongly reminiscent of the *loci* method of the memory arts. Upon each rotation of the disk a new indexical relationship (a "key") is established. The relation between plaintext and ciphertext letters is mutable yet fixed, and ultimately, requires such a mechanism to explore its combinatorial vastness.

Figure XX: Cipher Wheel, *De Cifris*

Aemulatio, analogy, and sympathy in Trithemius' magical cryptography

Compared to *convenientia,* the three other resemblances (*aemulatio*, analogy, and sympathy) are alike and yet conceptually quite different from the memory technologies we saw associated with *convenientia*. Foucault describes *aemulatio* as "a sort of convenience [that is, *convenientia*] that has been freed from the law of place and is able to function, without motion, from a distance," the "means whereby things scattered

[94] Kahn, "On the Origin of Polyalphabetic Substitution." Kahn does not describe what "horizon" device of Alberti's he is referring to. As we saw above, the *Descriptio Urbis Romae* shares more than a little conceptual lineage with the cipher wheel. Nonetheless, as a more distant source of inspiration I find Kahn's suggestion compelling.
[95] A modern English version of Lull's *Ars Brevis* is available in Llull, *Doctor Illuminatus*.
[96] There are several figures to Lull's art, and they developed during his prolific career. In the *Ars Brevis* the first, second, and fourth figures are circular, although the first figure bears the greatest similarity to Alberti's cipher wheel.
[97] Llull, *Doctor Illuminatus*, 301.
[98] Ibid., 303.
[99] Ibid., 298.
[100] Another potential source for Alberti's cipher wheel is the façade design for Alberti's Santa Maria Novella. In the Santa Maria design the disk is divided into 24 slices, although there is no rotating part or indexical relationship between marks; Williams, March, and Wassell, *The Mathematical Works of Leon Battista Alberti*, 195. Nonetheless, Williams seems to prefer this Santa Maria Novella explanation because it is more thoroughly mathematical (the 24 radii are composed on mathematical principles), but such an explanation presupposes a mathematization of cryptography that was largely absent prior to the nineteenth century, and has only come to dominate recently.
[101] Alberti, "De Componendis Cifris," 181 (xiii).

through the universe can answer one another," and a duplication within a mirror that "abolishes the distance proper to it."[102] Analogy is the old theory of mimesis but given the powers of universal application, drawing together the entire universe as a superimposition of *convenientia* and *aemulatio*. Analogy makes comparisons possible, like the mirroring made possible by *aemulatio*, but along with its inversion. Both *aemulatio* and analogy draw the universe together but only analogy places Man in the privileged point, capable of saying that "the plant is an upright animal" with its inversion "the root in the lower part of the plant and the stem in the upper part, for the venous network in animals also begins in the lower part of the belly, and the principal vein rises up to the heart and head."[103] Man is the "fulcrum" upon which these relations turn.[104] And finally, sympathy is a "principle of mobility" in that it attracts like things together: roots towards water, sunflowers to the sun.[105] Foucault notes that sympathy is an instance of the "Same" so strong and so insistent that it displaces likeness, a power of assimilation that renders things identical.[106] Natural magic made good use of sympathies, as for instance a tooth and a pinecone share resemblance and therefore share interior qualities capable of standing in for one another. Or, as Foucault describes, that "aconite will cure our eye disease, or that ground walnut mixed with spirits of wine will ease a headache," and that "there must of course be some mark that will make us aware of these things."[107]

In his exposition of Foucauldian method, Agamben reminds us that book nine of Paracelsus' treatise *De natura rerum* is titled "De signature rerum naturalium" (Concerning the Signature of Natural Things).[108] Paracelsusian epistemology finds that Nature does not "release anything in which it has not marked," as though the interior is visible from the exterior.[109] The key notion is the signature; the signature "is the science by which everything that is hidden is found."[110] Foucault writes: "There are no resemblances without signatures" and knowledge of resemblances is based on identifying and deciphering signatures.[111] The web of resemblances stand in need of signatures, offering the marks so that we know how to identify various resemblances.

Our point of reference for the three resemblances in the history of cryptography is Johannes Trithemius' (1462 – 1516) two cryptographic works, the infamous *Steganographia* and the sanitized *Polygraphia*.[112] The *Steganographia* was known while still being written and circulated as a manuscript before its posthumous publication in 1606, bundled with a "key" or *Clavis* written by Trithemius himself. The third book of *Steganographia* was never finished, but the manuscript was deeply sought.[113] After accusations of demonology, initially by the colleagues of Arnoldus Bostius,[114] Trithemius scuttled the project

[102] Foucault, *The Order of Things: An Archaeology of the Human Sciences*, 21–22.
[103] Ibid., 24.
[104] Ibid., 25.
[105] Ibid., 26.
[106] Ibid.
[107] Ibid., 29.
[108] Agamben, *The Signature of All Things*, 33.
[109] Ibid.
[110] Ibid.
[111] Foucault, *The Order of Things: An Archaeology of the Human Sciences*, 29.
[112] The most extensive description of Trithemius' *Steganographia* is only available in German: see Ernst, *Schwarzweisse Magie. Der Schlussel Zum Dritten Buch Der Steganographia Des Trithemius.*
[113] John Dee had managed to copy half of the manuscript and unsuccessfully offered "a Thouwsand Crownes" for the rest; Shumaker, *Renaissance Curiosa*, 97.
[114] In 1499 Trithemius wrote to his friend Bostius, but by the time the letter had arrived Bostius had died. His colleagues read the letter and seeing Trithemius' boasts of what the *Steganographia* was capable of laying clear accused him of being either a liar or a demonologist. See Reeds, "Solved: The Ciphers in Book III of Trithemius's Steganographia," 293.

and took to writing a version titled *Polygraphia* (1518), which was largely free from intermediating spirits.[115] Later (about 1503-04), the French mathematician Carolus Bovillus visited Trithemius and read some of the incomplete *Steganographia*.[116] In a 1509 letter Bovillus accused Trithemius of demonology, and when the letter was published a year later Trithemius' reputation for working with dangerous spirits was firmly established. At his death six years later, Trithemius was still denying his dogged reputation.

Despite its associations of demonology, many future cryptographers endeavored to harness the lessons of the *Steganographia*. "Gustavus Selenus" (pseudonym of Duke of Brunswick-Lüneburg, 1579 – 1666) wrote his *Cryptomenytices* (1624) with liberal quotations from three versions of the *Steganographia,* even going so far as to print the entirety of book three hoping that some future cryptographer might be able to supply a cryptological solution.[117] Similarly, Gaspar Schott (1608 – 1666) devoted two sections of his *Schola steganographica* (1655) to interpreting Trithemius' challenging work. In a more straightforward manner, and free from the associations of demonology, the *Polygraphia* also inspired many future cryptographers, including Giovanni Baptista della Porta's famous *De furtivis literarum notis, vulgo de zipheris, libri quinque* (1602).

Trithemius' introduction to cryptography may have arose from his hunt for manuscripts for the massive Sponheim library he developed (numbering almost 2000 volumes).[118] At a time when printing was rapidly advancing Trithemius was famously prickly about the technology, writing in his *In Praise of Scribes* that printed books were made of paper and "will disappear quickly," unlike the parchment manuscript (despite this, his *Polygraphia* was the first printed cryptography manual).[119] In one book buying expedition Trithemius encountered an old work on Tyronian notes in a Benedictine library, which he acquired for exchange of a new manuscript of St. Anselm's. Although really a form of shorthand writing used by Cicero's secretary, Tyronian notes were considered a form of cryptography. As was common for cryptography manuals of the time, Trithemius included a history of the subject in the *Steganographia* and *Polygraphia*, starting with both Tyronian notes and the Caesar substitution cipher, and elaborating on the origins of language.[120]

The first two books of the *Steganograpia* offer a fairly straightforward discussion of coded language, couched within examples of spirit conjurations. Shumaker offers the following example and interpretation (taken from the 1606 *Clavis*):

> *Pamersiel **A**noyr **M**adrisel **E**brasothean **A**brulges Itrasbiel*
>
> *Nadres **O**rmenu **I**tules **R**ablon Hamorphiel*

Shumaker indicates that if we ignore the first and last words (known as "nulls" which are inserted to help obfuscate the message), we can decode the message by reading alternate letters (here in bold type). The message is thus: "Nym die ersten Bugstaben de omni uerbo" ("Take the first letters of every word").[121] In the remainder of the first two books Trithemius offers other examples of coded language, some with more

---

[115] Ernst offers a careful description of the complicated manuscript and publication history. The *Steganographia* was actually composed of three parts, with a separate manuscript as an early version written between December, 1498 and March, 1499. The *Clavis* attached to the 1606 printed version bears resemblance to an earlier *Clavis specialis*, written after March, 1499 and discontinued in April, 1500. Furthermore, whereas the *Clavis specialis* contained plain-language descriptions of the cryptographic processes, when included in the *Steganographia* these parts were reworked into a kind of "arcane" language. See Ernst, "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia," 319.

[116] Ernst gives the date as 1503-04, but notes that it is unclear. See Ibid., 320.

[117] Shumaker, *Renaissance Curiosa*, 100; Reeds, "Solved: The Ciphers in Book III of Trithemius's Steganographia," 295. See also Strasser, "The Noblest Cryptologist."

[118] Grafton, *Worlds Made by Words*, 62.

[119] Ibid., 56; Reeds, "Solved: The Ciphers in Book III of Trithemius's Steganographia."

[120] Shumaker, *Renaissance Curiosa*, 94, 112.

[121] Ibid., 104.

complicated encodings of the same basic pattern (including the use of a single-alphabet substitution cipher). The *Polygraphia* also uses a transposition cipher, even (in book five), introducing a cipher wheel similar to the Lull-cum-Alberti invention from several decades prior.[122] And, like Alberti's invention, the *Polygraphia* uses a true polyalphabetic cipher (unlike the *Steganographia*, which only realizes a partial polyalphabetic cipher). As in the *Polygraphia*, in the first two books of the *Steganographia* the spirit names invoked are not "functional," rather they provide the "key" as a kind of password to decoding the messages. It is the third book of the *Steganographia*, not included in the 1606 printing and not part of the *Clavis,* that earned Trithemius the accusations of demonology. The third book includes many discussions of spirits and planetary intelligences, and remained undeciphered and utterly confusing well into the twentieth century. Even Shumaker's work, published in 1982, had to make due with a guess about the "true" contents of the third book.

In the late 1990s two scholars independently "cracked" the third book of the *Steganographia*, showing how, like the first two books, despite vivid discussions of spirits and planetary intelligences there is a solid use of cryptography, putting to rest the accusations, according to these authors, that Trithemius had any demonological intentions.[123] The third book contains eight tables of numbers grouped by the names of twenty-one planetary spirits or "rulers," each column containing data necessary for computing the position of the specific planet. To communicate secretly and swiftly without using human messengers, but by "natural" means, Trithemius insists, one must first use the data in the table to calculate the position and course of the appropriate planet. Then an image of the appropriate spirit is drawn on one piece of paper along with the name of the recipient, and on another piece of paper the process is repeated replacing the recipient's name with the message to be transmitted. The message itself must not violate a number of prescribed rules, such as being of a loftiness of purpose, or, important for our purposes, suffer from lack of clarity. Trithemius states that the correct notation, or "character" must be used to attract the appropriate spirit, otherwise the spirit may "refuse to obey."[124] This means, above all, identifying the correct astrological notation. Once complete, both sheets are brought together and placed in a special box, and within twenty-four hours the recipient will receive the message. Other sequences and descriptions in the third book can be decrypted in a manner similar to the first two books.[125]

With these fabulous descriptions of communication aided by spirits many scholars believed that the third book did not contain any cryptographic content, and was instead purely demonological. The most authoritative modern voice holding this position was D.P. Walker in his *Spiritical and Demonic Magic from Ficino to Campanella*, published as part of the Warburg Institute's revival of interest in magic and occult studies. Similarly, Nicholas H. Clullee claimed in his book *John Dee's Natural Philosophy Between Science and Religion* that there could not be any cryptography in the *Steganographia's* third book because it would be a conceptually unnecessary addition, since Trithemius indicated that the spirits transmit the messages directly. Ernst and Reeds showed that it does contain cryptography, but this does not mean that it conceptually excludes the spiritual exercises.

The spiritual exercises of the third book of the *Steganographia* function through the web of resemblances, folding the human and divine universes within. The spirits and planetary intelligences function to draw the mind away from changing particulars and towards universals. In Agrippa's *De occulta philosophia*, a product of Trithemius' counsel, his analogous method is intended to "proceed towards high things" and turn the mind "confidently to universals."[126] For miraculous phenomena, which all people in the sixteenth

[122] Ibid., 112.
[123] Ernst, "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia"; Reeds, "Solved: The Ciphers in Book III of Trithemius's Steganographia."
[124] Brann, *Trithemius and Magical Theology*, 138.
[125] Both Ernst and Reeds offer descriptions of the decryption process, in addition to their personal account of cracking the code; Ernst, "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia"; Reeds, "Solved: The Ciphers in Book III of Trithemius's Steganographia."
[126] Shumaker, *Renaissance Curiosa*, 109.

century believed to exist, the senses are insufficient for attaining knowledge. Magic and assistance from spirits were thus inextricably linked to scholarship. Thus developed a science of wonder, unlocking the powers of the method of the *Steganographia* and its hidden natural forces. For purely communicative purposes, the ability to transmit messages at a distance without an intermediating material body is possible only with the assistance of mediating spirits. These conjoined processes of *episteme* and technical communication hinge on the resemblances of *aemulatio,* working at a distance without motion, and freed from place. The cryptographic process is able to bring distant things together, but only with the assistance of messenger spirits. On the other hand, the process of drawing an image of the planetary intelligence on a piece of paper, as Trithemius imagined, represented distinct from any *aemulatio*. Instead, the drawing deployed the resemblances of analogy, a superimposition of *convenientia* and *aemulatio.* Analogy reconfigures the old processes of mimesis—here the drawing of the planetary intelligence (which can be a rough sketch, and reused for other messages, according to Trithemius),[127] working as a kind of mirror between the drawn image and the intended recipient's mind. The final resemblance, sympathy, is perhaps the most pervasive through Trithemius' technical communication schemes. Trithemius suggests that appropriately prepared lodestones, ringed with letters akin to a cipher wheel,[128] can transmit instantly across vast distances through sympathetic qualities interior to the lodestones. Similarly, Trithemius reports, after two people rub together the blood from cuts on their arms they will be able to communicate through sympathetic pin pricks, through a kind of global vascular Morse code.

While Reeds and Ernst have unequivocally proven that the third book of the *Steganographia* contains what we would consider cryptography, it is not the case that the invocations of spirits and planetary intelligences have nothing to do with the cryptography present, and nor does it mean that when Trithemius claims to use only "natural" means for communication that he intends this to be exhaustive of the cryptographic processes Reeds and Ernst eventually uncovered.[129] In fact, as we will see in more depth in Part 2, the invocation of angelic spirits are a useful theoretical concept for how the mediatic process of encryption occurs.

The key to understanding why Trithemius invoked spirits, and yet insisted that he did so "naturally" lies in his conception of nature. For sixteenth century occultists like Trithemius, nature was not a binary of the supernatural and natural, as we might believe today. Instead, as Daston has persuasively argued, there is a third category of being, technically part of nature but occupied by higher created beings, such as angels and spirits.[130] Daston remarks that in Augustine's conception of nature, all created being stemmed directly from God. According to Augustine, all nature, but especially the miraculous, was supernatural. Thomas Aquinas introduced an important change to Augustine's view. He saw that within nature there is a distinction to be made between the natural that occurs with regularity and order, and the natural that occasionally occurs. Some miracles may be strictly outside of the understanding of humans, and thus belong properly to the supernatural world, but other phenomena may be the result of natural processes. Marvels and the actions of spirits occur rarely, but are the result of created beings and thus (with difficulty) can be understood by humans. Spirits are created, but special beings—they are "preternatural." So, for Trithemius, invoking spirits to assist with his cryptographical activities is still, as he insisted, "natural" because the beings employed and the resulting phenomena were rare and difficult, that is preternatural, but in no way supernatural.

---

[127] Ernst, "The Numerical-Astrological Ciphers in the Third Book of Trithemius's Steganographia," 323.
[128] See also Brann, *Trithemius and Magical Theology*, 145.
[129] Reeds writes that "the cryptographic techniques are purely natural" and are only "disguised by the use of a figurative language of demonology," and that "the *Steganographia* can no longer be regarded as one of the main early modern demonological treatises but instead stands unambiguously revealed as the first book-length treatment of cryptography in Europe." Ernst appears to be much more careful about recognizing the historical context in which Trithemius was writing, noting that spirits and fabulous media technologies were commonplace and, in the minds of the authors of the day, necessarily part of cryptography.
[130] Daston, "Marvelous Facts and Miraculous Evidence in Early Modern Europe."

For Trithemius the spirits were wonderous media. Wonder is the touchstone of philosophical knowledge, the epistemic crux of universals not particulars. His designs for technical communication surpassed the limitations of material communication, but did not work as though by magic without an intermediating medium. Spirits work between the processes of cryptography as part of a technical form of communication, each necessarily in concert with the other. The transmission process extends writing, as it requires special performances and careful calculations, which, Trithemius suggests, it is a special part of grammar—not outside of writing, but rather a refinement and extension of writing.

Such an extension of writing is not usually part of contemporary discussions of media because theories of speech and writing existed long before the theorization of media in the twentieth century. The very idea of media precludes that which came before. Media are special, and modern, in ways that speech and writing are not.[131] And besides, according to conventional wisdom we have perfectly good theories of speech and writing, namely, the mimetic theory. As Guillory points out, the philological record indicates that the old term "medium" did not come to be connected with matters of communication until quite recently. As we saw previously, in Guillory's opinion, the concept of a medium of communication was "absent but wanting" for several centuries prior to its appearance.[132] The cause of this lacuna was, it seems to me, the powerful effect that Plato and Aristotle's theories of mimesis held. Only when the proliferation of new technical media proved too obvious to ignore would the term "media" finally emerge as a term of communication.

Turning back to plaintext, we can begin to see that mimesis isn't so much wrong as it is a distraction, an exhausted theory incapable of fully explaining many of the more recent shifts brought about by computer technologies. This theoretical exhaustion has left a vacuum in its place, as we struggle today to conceptually understand computational technologies. Until very recently the mimetic theories were believed to offer perspicuous descriptions of art, language, craft, and design. Even in our post-modern world, full as it is of computers and algorithms, mimesis is often the default position.

Today's computational technologies provide unparalleled technical capabilities but to ask simple questions about what they are is to invite many competing (and non-complementary) claims: computers are Turing machines, formal symbol manipulators, algorithmic processors of complexity classes, and so on. Paradoxically, these discussions have traditionally excluded discussion of media—only (some) so-called theories of "new" media give countenance to the mediatic form of computational resources. Plaintext is a very old "new" media, and an important part of a long developing notational discourse network.

The development of the notational discourse network arises from a fracturing mimetic theory. The cracks first begin to show in the long Renaissance. In the thirteenth century Ramon Lull's rotating wheels influence Alberti's cipher wheel in the fifteenth century, both of which run counter to mimetic arts. With each passing year the powers of cryptography grow and expand and turn further inwards to their notation. It is worth quoting Foucault's commentary at length, since his discussion precisely articulates this shift away from "resemblance" (née mimesis):

> *Up to the end of the sixteenth century, resemblance played a constructive role in the knowledge of Western culture. It was resemblance that largely guided exegesis and the interpretation of texts; it was resemblance that organized the play of symbols, made possible knowledge of things visible and invisible, and controlled the art of representing them. The universe was folded in upon itself: the earth echoing the sky, faces seeing themselves reflected in the stars, and plants holding within their stems the secrets that were of use to man. Painting imitated space. And representation – whether in the service of pleasure or of knowledge – was posited as a form of*

[131] Early media scholars, such as McLuhan, extended their analysis to print, and by some extension to writing, but rarely to speech itself. Only in very recent years has the term "media" been opened up to include broader phenomena. The widest interpretation I know of is John Durham Peters' recent work *The Marvelous Clouds*. Peters argues for an interpretation of nature itself as media.

[132] Guillory, "Genesis of the Media Concept," 321.

> *repetition: the theatre of life or the mirror of nature, that was the claim made by all language, its manner of declaring its existence and of formulating its right of speech.*[133]

Indeed, everything changes at the beginning of the sixteenth century. Francis Bacon develops a simple and rather forgettable cipher. His cryptographic invention would entertain later code hunters but fail to change the history of cryptography in any meaningful way. Then, despite its limited direct influence, the cryptographic idea plants a seed. Within a few decades of his youthful invention, Bacon develops a proposal for an artificial language of vast power: a notational media capable of spanning place and time, solving the challenges of scientific communication, and ultimately bringing all of humankind back under a single language to live in utopia. Developing an artificial language to solve these representational issues would stir the greatest minds of the next two centuries.

[133] Foucault, *The Order of Things: An Archaeology of the Human Sciences*, 19.