Unlocking the Digital Crypt: Exploring a Framework for Cryptographic Reading and Writing

Quinn DuPont
University of Toronto

Scholarly and Research Communication
VOLUME 5 / ISSUE 2 / 2014

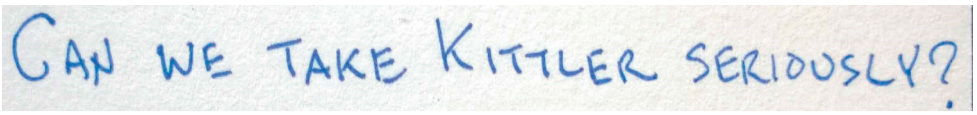
Abstract: This article argues that we should take seriously Friedrich Kittler's suggestion that we now live in a post-writing world. It is argued that much of this transition is due to the shift toward cryptographic writing. Shawn Rosenheim's *The Cryptographic Imagination* is briefly analyzed and critiqued; teasing out the many conceptual themes of cryptographic writing that Rosenheim presents, this article offers critique and analysis of his important work. As a way of rebuilding Rosenheim's analysis, an original conceptualization of cryptography is also briefly sketched. Returning to Kittler's suggestion, it is concluded that cryptographic writing performs an ordering role in our control society.

Keywords: Cryptography; Literacy; Digitality; Digital humanities

Quinn DuPont is a PhD Candidate in the Faculty of Information at the University of Toronto, 140 St. George St., Toronto, ON M5S 3G6. Email: quinn.dupont@utoronto.ca .

In "There is no software" Friedrich Kittler (1995) argues that the "last historical act of writing" occurred in the late seventies when the engineers of the Intel 4004 and then 8086 microprocessors unrolled 12 and then 64 square metres of blueprint paper to draw the electrical connections that were later optically reduced and etched into silicon. I take a pen and piece of paper and write**:**

Figure 1: JPEG image of author's holograph depicting "Can we take Kittler seriously?"



CCSP Press
Scholarly and Research Communication
Volume 5, Issue 2, Article ID 0502157, 8 pages
Journal URL: www.src-online.ca
Received December 12, 2013, Accepted January 11, 2014, Published May 9, 2014

Dupont, Quinn. (2014). Unlocking the digital crypt: Exploring a framework for cryptographic reading and writing. *Scholarly and Research Communication,* 5(2): 0502157, 8 pp.

I think we can. We now live in a computational world, but not in the vacuous sense of whirling media, interconnectedness, and repurposed telephone lines – Geert Lovink damns these analyses as "vapor theory" (in Galloway, 2006, p. 17). Instead, we have become a "slave to the algorithm" (Slater, 2013), where our interactions across space and time are computational (Takhteyev & DuPont, n.d.), our economy ordered according to alphabetic and machinic logic (DuPont, 2014), and so on.

Taking Kittler seriously, we ask, what is the new root (and route) of our computational age? Kittler points to code. But, this is not Umberto Eco's semiotic code (1986), rather it is the inscription that follows from typewriter to computer (Kittler, 1999). And long before the typewriter, the inscription was cryptographic (Kittler, 1995). With the introduction of the Intel 4004 microprocessor, writing ceased and was replaced with cryptographic inscription.

This article introduces an underappreciated domain of analysis for digital humanities. I argue that we should take seriously Kittler's suggestion that we now live in a post-writing world. I problematize a JPEG image to show how its reality is cryptographic. I then turn my attention to the best, and perhaps only, existing analysis of cryptographic writing, Shawn Rosenheim's *The Cryptographic Imagination*. By teasing out the many conceptual themes of cryptographic writing that Rosenheim presents, I offer critique and analysis of his important work. I briefly suggest an original conceptualization of cryptography for our age, but show how other conceptual themes may have been productive in their own ages. Returning to Kittler, I conclude by arguing that cryptographic writing performs an ordering role in our control society, quite distinct from natural, "human" (hand/) writing.

Speech, writing, printing, code, and cryptography

Figure 2: The first 100 bytes in hexadecimal encoding of the discrete cosine transformation (DCT) scan data from a JPG-compressed image portraying "Can we take Kittler seriously" in the author's holograph.

```
00 0C 03 01 00 02 11 03 11 00 3F 00 F4 0B B2 B1 F1 DA 1D 7B C5 61 D3
B4 41 24 C6 AE DA CA F7 3F D9 F9 FE DF 62 35 6F 65 8C 6B EB 70 B1
8E 01 CC 73 48 70 70 3A B5 EC 73 7D AE 6F EE AA B5 58 DA AE CC BA
C3 B5 D5 16 EE 71 06 5B 40 AD B6 32 36 FB BD 3F 53 ED 0F FF 00 8C 42
BB A9 B3 17 2D F8 E5 BB AB AE 8D ED AA A6 12 ED DB 6C B9 8D 6B
9B FA 1D 97 55 4B EB AA BF F4 CC FF 00 84 4F E0 27 40 09 35 6B 78 AB
73 E0 E9 80 7C 3E 29 C7 E4 EC 15 5C 1C A6 64 D4 EB 19 63 6D
```

Figure 1 is an image of failure. Despite my efforts, I have answered Kittler's charge not with a written answer, but with code (Figure 2). This code represents the raw discrete cosine transformation (DCT) scan data from a still image conforming to the ISO 10918-1 (JPEG) standard. Prior to the Start of Scan (SOS) JPEG marker FF DA (elided here), the image file contains Exchangeable image file format (Exif) metadata about the image, its creation, and so on. Once the Exif metadata is re-encoded from binary to American Standard Code for Information Interchange (ASCII) English text, it shows

Dupont, Quinn. (2014). Unlocking the digital crypt: Exploring a framework for cryptographic reading and writing. *Scholarly and Research Communication,* 5(2): 0502157, 8 pp.

the traces of human language**:** Nokia.Lumia 920...ü€..'...ü€..'..Adobe Photoshop CS6 (Windows).2013:08:29 10:27:22.

The Exif data shares sense and sensibility with software source code, for example, it vaguely resembles the now-famous Commodore routine *10 PRINT CHR$(205.5+RND(1)); : GOTO 10* (Baudoin, Bell, Bogost, Douglass, Marino, Mateas, Montfort, Reas, Sample, & Vawter, 2013), at least to the extent of being interpretable by humans. Software source code, however, bears little resemblance to the DCT scan data that follows (Figure 2). The DCT scan data is not just (source) "code," rather it is cryptographic.

I argue that while we need tight constraints on what we are willing to call "cryptography," cryptographic writing needs to be understood more broadly than just the application of "real" (or secret) cryptography to "human" texts. One of the more recent famous examples of cryptographic writing is *Agrippa (a book of the dead)* (Ashbaugh, Begos, & Gibson, 1992). In this work, Gibson's poem was encapsulated in an interesting software application that utilized a rough approximation of off-the-shelf cryptography (DuPont, 2013; Hehmeyer, Hodge, Kirschenbaum, Knight, Liu, Roh, & Swanstrom, 2005). Deeper analysis revealed that *Agrippa* never really managed to accomplish "good" secrecy, as usually intended by these industrial cryptographic algorithms – but this is surely not the point. The rhetorically similar JPEG encoding shown above is also not intended for secrecy. While *Agrippa* is a provocative example and surely counts as cryptographic, we need to think somewhat more expansively to see the rest of the plethora of cryptographic works in our midst.

In order to get the idea of cryptographic writing going, we need to discard with narrow definitions, usually motivated by scholars in the computer engineering field. While the classical definition of cryptography is "information secrecy" (Shannon, 1949), this cannot evacuate the rich use of cryptography outside of computer engineering. We must realize that (computerized) secrecy is but one possible conceptualization, and while it is vastly in the majority, other conceptions are possible.

The history of cryptography also reveals a plethora of uses of cryptography. David Kahn (1967) provides the *locus classicus* for the history of cryptography and hews closely to secret uses of cryptography. There is, however, a kind of untold, alternative history that has unfortunately received very little attention. Even a fleeting discussion of the untold history, as told below, is illuminating of the diversity of uses. Renaissance authors such as Athanasius Kircher saw cryptography as a tool for the investigation of the natural world (literally reading the "Book of Nature"). Cabalistic influences, both mystical and practical, dominated discussions of cryptography throughout modernity, including G.W. Leibniz's *De Arte Combinatoria*. Francis Bacon's biliteral cipher straddled secret and scientific uses. John Wilkins' exploration of encyclopedic and universal knowledge in his *Essay* developed thoughts first worked out in his cryptography manual *Mercury*. The role of cryptography in the formation of the Modern mind is sadly unappreciated and poorly understood, but can only be gestured at here.

Cryptographic writing part 1: E.A. Poe

If we are willing to say that any encryption is cryptographic writing, then increasingly its use is commonplace. Cryptography is now explicitly used in a great deal of communication on the Internet, and software developers routinely cry "encrypt everything!" as a panacea to the woes of government snooping and criminal hacking (see Cardozo, Higgins, & Opsahl, 2013). The traditional field of cryptography – part computer science, part mathematics – is burgeoning and widely recognized as extremely important. Yet, while this research is very good at operationalizing encryption, calculating computational "hardness," and inventing new and more secure methods, very little attention has been paid to the conceptual underpinnings of cryptography. When cryptographic writing is intentionally artistic – in poetry, new media, art, and literature – the lines blur even further.

Shawn Rosenheim's *The Cryptographic Imagination* (1997) tackles the issue of cryptographic writing head on. Through a detailed analysis of E.A. Poe, Rosenheim persuasively argues that "cryptographic imagination" lies behind huge swaths of Modern literature. This work is certainly the best, if not the only, detailed monograph on cryptographic writing. I identify some of the major conceptual themes in *The Cryptographic Imagination* and offer a critique and evaluation, in hopes that I may be able to take the richness of Rosenheim's work and generate a somewhat more schematic and analytical conceptualization of cryptographic writing. As I see it, Rosenheim identifies the following conceptual themes of cryptography: secrecy, syllabification, conventional versus essential signification, mimetic transmission of information, and doubling of signs.[1]

Secrecy: Drawing on the dominant conceptualization of cryptography (as mentioned above, with Shannon), Rosenheim (1997) describes cryptographic writing as "secret" and semiotically "illegible" (p. 21). When it comes time to discuss modern digital images, Rosenheim turns to the secret nature of steganography (or hidden writing, the cousin of cryptography) to articulate its inner logic. This conceptual apparatus creates trouble when drawn backwards into history; it makes strange the rich non-secret history of cryptography, from ancient times to Modernity. Additionally, secrecy is a wily, ill-formed notion that relies heavily on authorial intention – a matter that humanists ought to be very sensitive about deploying in any analysis, as New Criticism has taught us so well. The questions arise: when writing cryptographically who keeps the secret, and it is kept secret from whom? Secrecy is surely part of some cryptographic writing, but this shifting, socially articulated phenomena is, I argue, too unstable to rest on.

Syllabification: To make a point about the linguistics of cryptography, Rosenheim's Poe juxtaposes a sailor and an ape, who share even in the "wildest paroxysms" a coherence of syllabification (p. 73). Here, the sailor and the ape do not share cryptographic writing, but instead what Rosenheim calls an "aural cryptogram" (p. 73). Yet intuitively, the very existence of a spoken cryptogram is problematic. Poe's own work drives home the issue: in the audio book version of *The Gold Bug* (Poe, 2013) the narrator has to comically *voice* the cryptogram on Legrand's sheet of paper, resulting in a long passage of "five, three, double dagger, double dagger, single dagger, three, zero… ." The lie that aural cryptograms perpetrate is that cryptography could maintain the

Dupont, Quinn. (2014). Unlocking the digital crypt: Exploring a framework for cryptographic reading and writing. *Scholarly and Research Communication,* 5(2): 0502157, 8 pp.

necessary semiotic distance to still be called cryptography without simply collapsing into natural language. It seems that, unlike natural language, cryptography cannot "directly" signify the world (otherwise, where is the "secret" or other semiotic shift?).[2] As an example of this rapid collapse into natural language, one could argue that Pig Latin is a kind of encryption (it performs substitutions and transpositions on written language). So, once a community (or audience) becomes proficient at mentally rearranging the letters for "decryption" Pig Latin ceases to be cryptography, and instead becomes a new language (albeit a pidgin language).

Conventional versus essential signification: How cryptographic symbols signify is a perplexing and long-debated issue. Coming down on *both* sides of a historical debate, Rosenheim's Poe (paradoxically) argues for both the conventional – or constructed – nature of signs (a modern phenomenon, according to Rosenheim, p. 23), and the essential, originary nature of signs (p. 53). In fact, far from being a Modern (or postmodern) position, the idea that the signifier has no essential relationship to the signified has long been debated. When working through linguistic and cryptographic ideas, Francis Bacon (1561–1626) argued for the conventional nature of signs (an insight that helped move his analysis away from the mystical, essentialized signification of Renaissance cryptographers). On the other hand, Rosenheim's Poe describes hieroglyphs as perfect or originary language, admitted to be a "specious move" according to Rosenheim, but extremely common in the history of language. Like Poe (Rosenheim, 1997, p. 53), Athanasius Kircher (c. 1601–1680) saw the world as text (capable of being literally read as the "Book of Nature"). This debate later came to head in the so-called "crisis of representation" (Markley, 1993), which played out with the universal and philosophical language planners (Maat, 2004).

Mimetic transmission of information: Articulating a conception of media that has long been influential, Rosenheim's Poe argues that cryptographic writing constitutes the mimetic transmission of information. Both the daguerreotype (and other imaging technologies, p. 95), and the invention of the telegraph (p. 89) are seen as a form of cryptographic writing that will usher in the death of distance (see Takhteyev & DuPont, n.d. for a critique of such arguments.). Perplexingly, this prosthetic transmission is not just corporeal; recalling Renaissance media experiments (Zielinski, 2008) with camera obscuras and auditory mechanisms, Poe argues that cryptographic writing extends to the dead through the use of telepathic mediums that unlock the crypt of the soul (p. 115). In contrast, while cryptographic writing can be fruitfully understood as communication, it can also be used post-mediatically as data for computation. Additionally, cryptographic writing fails as a form of mimetic representation. Despite Poe's claims of "intuitively" understanding the logic of cryptograms, cryptography resists total comprehension. Unlike mimetic representation, understanding (cryptanalysing) cryptographic writing requires decomposition into parts, otherwise the work stays smooth and opaque. Any code-breaker will describe how non-trivial cryptanalysis is an analytical, step-by-step process, not sudden intuition.

Doubling of signs: Distinguished from natural language, Rosenheim's Poe argues that cryptographic writing is a doubling of signs (p. 30), evocatively suggesting an interpretation of language as script (p. 52, 74). Although Rosenheim's Poe waffles on the details of what is doubled (at times the signified is doubled into two signifiers, or at

times the signifier is doubled), he is surely on the right track. The right doubling, I argue, is the derivative substitution of a signifier for another signifier. To employ Poe's example, the face card is not a doubling of the (human) face, but in cryptographic writing the face card is replaced with another face card.

Cryptographic writing part 2: Toward second-order notational systems

Rosenheim offers many themes for the conceptualization of cryptography, but it is clear that there is no one, univocal way forward. Not all themes are commensurate (conventional versus essential signification), and many fail immediately when subjected to cursory analysis (syllabification of cryptography). Other themes are historically particular and not appropriate for our age (or in Foucauldian inflection, "*episteme"),* because we no longer hold the necessary worldviews (mimetic, mediatic cryptography). The remaining themes provide a good foundation for some analytical reworking: 1) Secrecy is often part of cryptography, but not exclusively so, and should not be relied on for precise analysis. 2) Semiotic doubling occurs from signifier to signifier, not from the problematic doubling of the signified.

I have begun developing a framework for cryptography elsewhere, which, to avoid a very long digression, will only be hinted at here.[3] I argue that cryptography can be understood as a second-order code, where "code" is understood in terms of Goodman's notational system (1976). For Goodman, a notational system must be disjointed (equivalent inscribed marks – tokens – must be interchangeable), differentiated (different inscribed marks must be able to be distinguished from each other), and unambiguous (each inscribed mark must symbolize only one thing). As also suggested by Rosenheim's Poe, I argue that cryptography doubles these notations, so rather than connecting a signified to a signifier (in Goodman's original analysis), cryptography doubles the signifier. Further, cryptographic *writing* goes one step past a doubled notational system, like a computerized *encryption* process, cryptographic writing is a performance of this special code (and thus, a particular cryptographic writing – "writing" as a verb – is said to be a performance of a particular work, just as the London Philharmonic *performs* Beethoven's *work*).

I argue that the only way to understand the diversity of cryptography is to adopt a historically realist methodology. Therefore, it is worth underlining that cryptography is not trans-historically stable. The framework above models our current *episteme*, roughly delineated by Kittler's discourse network "1900" (1990). Although technologically driven, cryptography is not historically linear, and other ages may share the themes discussed above (and while I may have critiqued the themes as being analytically problematic, many were highly effective in their own age). Nonetheless, investigating our current conception of cryptographic writing exposes its ordering effects on *our* techno-social reality.

Ordering machines in the control society

Returning to Kittler's initial problematic, how can we understand cryptographic writing after the age of writing? Above, I briefly argued that the mimetic media effects of cryptography belong to a previous era. The discrete nature of cryptographic marks resist mimetic representation (properties commonly called verisimilitude, realism, or likeness). The cryptographic code of the JPEG above is the real, and the mimetic

Dupont, Quinn. (2014). Unlocking the digital crypt: Exploring a framework for cryptographic reading and writing. *Scholarly and Research Communication,* 5(2): 0502157, 8 pp.

depiction of the printed words is simply the contingent reassembly of the code. Without the complicated assemblage of working technologies, policies, standards, and tacit knowledge, the mimetic properties of the JPEG image would simply cease to exist, leaving the trace of a code to be cracked for future generations.

For the same reason that we must reject Poe's mediatic decryption of the soul (if the soul is a crypt, it remains locked in our scientific age); we must reject a mediatic gloss for cryptographic writing. Our cryptographic *writing* is necessarily a digital notation, most accurately *read* by way of media archeology (Ernst, 2013; Kirschenbaum, 2008; Parikka, 2012). I argue that the most powerful effects of computation are not due to mediatic uses (e.g., using a computer as a doppelganger for a television or radio), instead, computed and therefore *ordered* realities dominate. We can name these technologies by their cause (algorithms) or their effect (order). The performance of these ordering technologies is ground zero for the shift to a control society (Deleuze, 1992) – our coming reality.

Cryptographic writing shares with natural, "human" (hand/) writing in that it is representational, but only available in a post-human or god-like register of meaning, since cryptographic writing stymies human intuition. Also like natural writing, cryptographic writing orders the world (and self) in particular ways (a fact that makes the invention of writing – and cryptography – so powerful and influential). Cryptographic writing, unlike natural writing however, has the potential to represent and order in devious, unseen, and potentially more powerful ways. As an art form and a root of scientific knowledge – and not just secrecy – cryptographic writing holds immense potential, and begs for more scholarly analysis.

Notes

1. I distinguish between what might be called "cryptic writing" and "cryptographic writing." Often, as I am sure Rosenheim is fully aware, Poe and the other characters in *The Cryptographic Imagination* are engaging in cryptic writing, a loose constellation of mysterious, spooky, and metaphoric rhetoric. Cryptographic writing, on the other hand, can be productively compared to "real" cryptography (of the sort a computer scientist may recognize). The lines between "real" cryptography and "cryptographic writing" often blur.

2. Derrida's critique (1998) of the metaphysics of presence and logocentricism lurk behind the binary of written and spoken language and the mediations that they entail.

3. My PhD dissertation develops this line of analysis much further.

References

Deleuze, G. (1992). Postscript on the societies of control. *October*, *59*(Winter), 3–7.

Derrida, J. (1998). *Of grammatology*. (G.C. Spivak, Trans.) (Corrected.). Baltimore, MD: The Johns Hopkins University Press.

DuPont, Q. (2013). Cracking the Agrippa code: Creativity without destruction. *Scholarly and Research Communication*, *4*(13), 1–8.

DuPont, Q. (2014). The politics of cryptography: Bitcoin and the ordering machines. *Journal of Peer Production, 1*(4). URL: http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-politics-of-cryptography-bitcoin-and-the-ordering-machines [May 9, 2014].

Eco, U. (1986). *Semiotics and the philosophy of language*. Bloomington, IN: Indiana University Press.

Ernst, W. (2013). *Digital memory and the archive*. (J. Parikka, Trans.). Minneapolis, MN: University of Minnesota Press. URL: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=586190 [December 17, 2013].

Galloway, A.R. (2006). Protocol. *Theory, Culture & Society*, *23*(2–3), 317.

Gibson, W., Ashbaugh, D., & Begos, K.J. (1992). *Agrippa (a book of the dead)*. New York, NY: Kevin Begos Jr. Publishing.

Goodman, N. (1976). *Languages of art: An approach to a theory of symbols*. Indianapolis, IN: Hackett Publishing.

Kahn, D. (1967). *The codebreakers: The story of secret writing*. New York**,** NY: Macmillan.

Kirschenbaum, M.G. (2008). *Mechanisms: New media and the forensic imagination*. Cambridge, MA: MIT Press.

Kittler, F. (1990). *Discourse networks 1800/1900*. Stanford, CA: Stanford University Press.

Kittler, F. (1995). There is no software. *CTheory*, *32*. URL: http://www.ctheory.net/printer.aspx?id=74 .

Kittler, F. (1999). *Gramophone, film, typewriter* (1st ed.). Stanford, CA: Stanford University Press.

Liu, A., Hehmeyer, P., Hodge, J., Knight, K., Roh, D., Swanstrom, E., & Kirschenbaum, M. (2005). The Agrippa files. URL: http://agrippa.english.ucsb.edu [October 18, 2012].

Maat, J. (2004). *Philosophical languages in the seventeenth century: Dalgarno, Wilkins, Leibniz: Dalgarno, Wilkins, Leibniz*. Springer.

Markley, R. (1993). *Fallen languages: Crises of representation in Newtonian England, 1660-1740*. Ithaca, NY: Cornell University Press.

Montfort, N., Baudoin, P., Bell, J., Bogost, I., Douglass, J., Marino, M.C., Mateas, C.R., Sample, M., & Vawter, N. (2013). *10 PRINT CHR$(205.5+RND(1));:GOTO 10*. Cambridge, MA: MIT Press. URL: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=513654 [December 17, 2013] .

Opsahl, K., Cardozo, N., & Higgins, P. (2013, December 16). UPDATE: Encrypt the Web report: Who's doing what. *Electronic Frontier Foundation*. URL: https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what [December 17, 2013].

Parikka, J. (2012). *What is media archaeology?* Cambridge, UK; Malden, MA: Polity Press.

Poe, E.A. (2013). *The gold bug* (Unabridged.). Audio Books by Mike Vendetti.

Rosenheim, S. (1997). *The cryptographic imagination: Secret writings from Edgar Allen Poe to the Internet*. Baltimore**,** MD: The Johns Hopkins University Press.

Shannon, C. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, *28*(4), 656–715.

Slater, J. B. (Ed.). (2013). *Slave to the Algorithm* (Vol. 3). Mute.

Takhteyev, Y., & DuPont, Q. (n.d.). Ordering space: Alternative views of ICTs and geography. *Manuscript in Preparation*.

Zielinski, S. (2008). *Deep time of the media: Toward an archaeology of hearing and seeing by technical means*. (G. Custance, Trans.). Cambridge, MA: MIT Press.