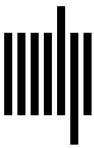
Cryptographic City

Decoding the Smart Metropolis

By: Richard Coyne

Citation:

Cryptographic City: Decoding the Smart Metropolis
By: Richard Coyne
DOI: 10.7551/mitpress/14712.001.0001
ISBN (electronic): 9780262374811
Publisher: The MIT Press
Published: 2023



The MIT Press

2 Write Me a City

If cryptography is hidden writing, then I need to establish that cities are already sites of plain text, in other words, ordinary language and unencrypted writing. In this chapter I will martial evidence that affirms the connection between place and writing. This provides a grounding for my case that urban and cryptographic affordances are related.

Urban Ciphers

Cryptography is an old practice embedded in the functioning of cities and nations. Generals and soldiers would pass messages up and down the chain of command in secret to avoid interception by an adversary. Writing in the 1600s, the English natural philosopher John Wilkins (1614–1672) affirmed that whether in a dungeon, a city under siege, or a hundred miles away "there are certain ways to discourse with a friend."[1] He was referring to cryptography and he recounted numerous methods for sending messages in secret, including examples of the kinds of short messages delivered by citizens and leaders under siege.[2] Epidemics and starvation were among the afflictions that beset a besieged city and required secret communications.

I am largely drawing this historical account from the book *A Cultural History of Early Modern English Cryptography Manuals* in which Katherine Ellison recounts the four-hundred-year history of secret messaging as a necessity, a hobby, and an obsession.[3] Wilkins's book of the 1600s is a prime example of one of these early cryptography manuals. As I will demonstrate in this chapter, secret writing dates to the dawn of language. By related accounts, people's interest in cryptography was amplified in the age of the printing press in the 1400s.

According to Ellison, in Wilkins's time cryptography provided "a promising solution for loneliness and survival in a disconnected world of local and global conflict."[4] Crossword puzzles, Sudoku, and Wordle are no doubt contemporary survivors of the recreational study of ciphers and cryptography. Solving puzzles, playing video games, posting on social media, and sending messages are common diversionary pastimes that fulfill similar appetites.

There is a complete facsimile version of Wilkins's *Mercury* at Google books and elsewhere. The full title on the book cover is *Mercury: Or The Secret and Swift Messenger. Shewing, How a Man may with Privacy and Speed communicate his Thoughts to a Friend at any distance*. The book explains that the most cunning methods of passing messages were those concealing to a potential interceptor that there is even a message in play. One method involved an innocuous knotted piece of string secreted around a saddle or threaded into clothing. When unfurled and zigzagged across a wooden template guided by side notches, the otherwise random knots line up against the letters of the alphabet to reveal the secret message. The message so derived in figure 2.1 says to "beware of this bearer who is sent as a spy over you."

Not all cryptographic methods were efficient. Wilkins recounts how the sender could shave the head of a young servant, then write something on the servant's scalp. When the hair had grown back the servant would be dispatched to the recipient, who would then shave the servant's head to reveal the message. Not all messaging techniques are instantaneous. Wilkins doesn't provide an example of the kind of message that would be so conveyed.[5]

Words and Places

Though cryptography pertains to all manner of secret communications via symbols, drawings, geometries, sounds, and movements it is most at home as an art of concealing text messages. Pioneer of digital media in architecture and urbanism, William J. Mitchell wrote extensively on the cultural nexus between digital technologies and the culture of cities. In his book *Placing Words: Symbols, Space, and the City*, Mitchell makes an astute observation linking text to place.[6] Where words appear in physical space really matters, he observes. Meaning relies on context, and location is a crucial aspect of the context in which words both spoken and written assume their meanings. He provides the example of the word *fire*. Uttered in a

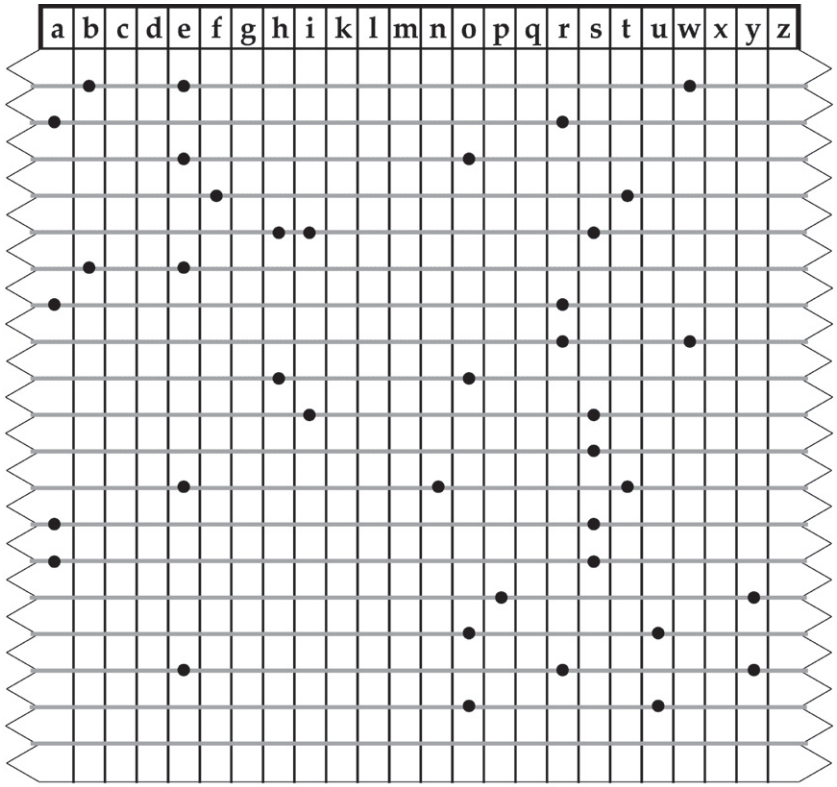


Figure 2.1
String cipher. When the string is unfurled and zigzagged across a wooden template the knots line up against the letters of the alphabet to reveal the secret message. Redrawn by the author from Wilkins's *Mercury* (1641), 46.

crowded theater it means something different than when uttered on a rifle range. Think also of the place dependence of signs, such as "No standing anytime." I have stumbled across several photographs online of someone standing on the shoulders of another person while clinging defiantly to a road sign that says "no standing on shoulder." Assuming you get the dual meaning of the word "shoulder," the joke here is achieved as if acting in defiance of the sign, as though the words belong in some other context, perhaps in a gymnasium.

The place dependence of word meaning already entitles architecture, planning, and urbanism to claim crucial roles in the way language works.

Mitchell describes the complicated relationships among people and things in the city as "intertextual": "So the vast web of intertextual relationships that we continually navigate in our intellectual and cultural lives is inextricably interwoven with the physical objects and spatial relationships that constitute the city."[7]

Physical signs, inscriptions, advertisements, and graffiti have their place—the places where they are meant to be read. Think of that place as their site of origin. What do digital communications do to the attachment of words to their origin? According to Mitchell, digital communications violate the claim that any particular word is grounded in a place. He wants us to consider what digital messaging does to words, contexts, and meaning: "the physical settings that we inhabit are increasingly populated with spoken words, musical performances, texts, and images that have been spatially displaced from their points of origin, temporally displaced, or—as in the case of email and Web pages downloaded from servers—both spatially and temporally shifted."[8]

He suggests here that the ungrounding of words to place is peculiar to the digital age. Contrary to Mitchell's account of the disruptive nature of digital communications, I advocate a counterargument that much of the power of words resides in their portability anyway. It has always been so, long before electronic communications. Followers of the philosopher Jacques Derrida would point readily to the contention that whether written or spoken, words move from one location to another, in the recounting of what someone said, memorizing and reciting prose, and as written down.[9] Rather than embark on a critique of words' dependence on place, I want to accept Mitchell's assertions as evidence that entitles us to discuss text and the city in the same breath, as it were. Texts, whether rooted in or uprooted from places, are part of the city. I also want to show how important mobility is in thinking about the shape of cities—not how people move about the city, but the city as a configuration of movable elements. Further on in this chapter I will talk about movable type in the printing process, but at this stage in the discussion I want to establish the various ways that text, writing, cryptography, and the city are related.

The quotes earlier on in this section were from Mitchell's last book on cities in a career cut short before cryptography came to the fore as a consideration in the smart city. But he observed in 2005 that under the sway of digital programming, the elements of a city can and will operate in much

the same way as someone speaking to you: "programmable objects can perform speech acts, and autonomously engage you in various forms of discourse. They can query you, demand information such as passwords, refuse you access, provide you with information, accept your instructions, and issue orders to you."[10] That communicative aspect of the city also harbors the potential for deception. These digitally communicative elements of the smart city can cause harm: "They can dispense facts, fictions, and lies. And malicious computer viruses, worms, and Trojan horses can take over networked, programmable objects to do you harm."[11] By this reading, texts in the city are implicated in the challenges of security, privacy, falsity, and verification, part of the language of cybersecurity and cryptography.

Other researchers align cities to writing, though under a more general category. Urban theorist Shannon Mattern sees the city through the category of *media*. She affirms the influence of writing, voice, text, printing, and the media in which they are expressed that include steel, stone, mud, clay, wood, and paper in the formation of cities. Cities have similarly influenced writing. She positions concepts of the contemporary smart city in this broader historical and cultural context: "today's smart cities don't have a monopoly on urban intelligence. In fact, we can trace that 'smart' genome all the way back to ancient Rome, Uruk, and Çatalhöyük."[12] Mattern is referring to the centers of Roman, Mesopotamian, and Neolithic influence.

The metaphor of city as medium is powerful in the context of cryptography, Mattern states: "For millennia, our cities have been designed to foster 'broadcast'; they've been 'wired' for transmission; they've hosted architectures for the production and distribution of various forms of intelligence and served as hubs for records-management; they've rendered themselves 'readable' to humans and machines; they've even written their 'source code,' their operating instructions, on their facades and into the urban form itself. They've coded themselves both for the administrative technologies, or proto-algorithms, that oversee their operation and for the people who have built and inhabit and maintain them."[13] Her reference to codes and algorithms helps ground further the framing of the cryptographic city.

There are other connections between writing and the city. Cities often confuse visitors, as if they harbor secret messages. The texts of any city are not always clear and unambiguous. Consider the challenge of reading and interpreting the artifactual remnants of a ruined city such as those of Rome,

Figure 2.2
Monte Albán, Valley of Oaxaca, Mexico. *Source:* Dmitry Rukhlenko via Shutterstock.

Uruk, or Çatalhöyük, especially where its inscriptions and graphic symbols are undecipherable. While researching cryptography in cities, I came across an article by Robin Heywarth about Monte Albán, the ancient Mexican city (figure 2.2). The article calls Monte Albán the "encrypted city." That phrase set me thinking about the extent to which any city can be so described. The ruins of Monte Albán are marked with so-far undecipherable symbols and markings etched into the stone fabric of this ancient city. The article also claims that the lines of the city's geometry are similarly coded: "Whilst the lines alone could be dismissed as meaningless . . . the numbers of proposed alignments add weight to the idea the city is encrypted with astrological information that would be easily deciphered by the High Priests of the city."[14] Ancient cities will inevitably appear as if in code, and encrypted, especially if they suffered decline or were destroyed before European scholars had a chance to tap into local memory pools. As I discussed in chapter

1, it is easy to regard hand-carved stone remnants as speaking from the past. But like the symbols in the ancient city of Monte Albán, digital cryptography writes itself across any city. Dare I say it even *writes* the city.

Shibboleths

Not only writing, but also the way things are said links text to places. You can tell where someone is from, or not from, by asking them to say a particular word. It can also indicate where someone has been. I can tell with a degree of certainty if someone has been to Australia by the way they say "Melbourne." If they draw out the final syllable, as it's written, then they have probably not said it often enough and in the right company to be "corrected" to say "Melb'n."

A shibboleth is a similar kind of pronunciation test. The word *shibboleth*[15] comes from a story in the Biblical book of Judges 12:6. The word simply means "the ear of a grain." When prompted to say "shibboleth," someone under suspicion wouldn't be able to pronounce it with the full "sh" sound as would a native speaker of the Hebrew dialect and so would give themselves away as the adversary. There's a spatial aspect to the use of words in this way. Words sound different according to where they are spoken and by whom. Dialect belongs to place. Something similar applies to vocabularies. The ancient Greek hero Odysseus was told to carry an oar from his ship with him to the center of the island of Ithaca.[16] When people he met started referring to the oar as a *winnowing fan* (for separating wheat from chaff), then he knew he was a long way from the ocean.

Some activists now recruit the word *shibboleth* to draw attention to racial and cultural division. *Shibboleth* was the name of an art installation by Doris Salcedo at Tate Modern in London in 2007. The artist hammered a big crack in the floor of the main exhibition hall. The crack has since been filled in with cement and rendered over to create a smooth but still visible trace. Doris Maria-Reina Bravo provides a helpful post explaining the naming of the work: "Every community, culture, and nation has its shibboleth. Among the U.S. military, 'lollapalooza' was used during World War II since its tricky pronunciation could identify native, English-speaking Americans. But the sinister history of the word 'shibboleth' illustrates how friends and enemies are separated by fine, linguistic lines. Any stranger in a foreign land appreciates the vulnerability this entails, especially the fear of being

outed as a foreigner and exposed in a hostile environment."[17] Here shibboleth stands for the displaced, the "out of place," and otherness.

Shibboleth is a prosaic word but sounds as though it should be the name of a monstrous creature. The name is adopted as such in entertainment and gaming.[18] It also crops up in online searches for academic papers. The word has caught on as a brand, notably in accessing academic texts online.[19] As with most words, the sound of the word contributes to its usage, nuance, and endurance. Pronounced "correctly," the word starts with the /sh/ sound that we use to instruct others to keep quiet. I will return to this thread in chapter 3.

Talking Trash

Ways of talking help define spaces. Like most urban commuters I have learned to tune out other people's mobile phone conversations. But when I'm forced to attend to a one-sided overloud conversation the interlocutor may as well be speaking in code: "She said that? . . . He did it then. . . . Ask him to give it to me when I'm there." *Deictic* utterances are those for which the listener needs to know the spatial and temporal context in order to establish meaning, and just hearing one side of a conversation makes it difficult to discover that context. It is in part a characteristic of grammar and how we use pronouns. Without the referent ("John," "the man in the seat opposite," "the boss"), "he" and "him" are insufficient to know who someone is talking about.

Competent language users are of course adept at speaking to one another in this coded way so that potential eavesdroppers would have to work hard to get the gist of the conversation. Avoiding proper names and other overt references to the subject matter is one way of "encrypting" the conversation. Another is to use abstruse terminology. In discussing this kind of coding I've drawn on themes developed in my 2010 book *The Tuning of Place*. There I focused on the mimetic and repetitive nature of arcane signals to claim space. Groups of friends would deploy vocal mimicry when they enter each other's company. In studying sound and the voice in the urban context, Jean-François Augoyard and Henry Torgue noted how teenagers' conversations are often filled with "onomatopoeia, interjection, and deictic words borrowed from the media or cartoons."[20] The listener needs to know the context in order to ascertain any meaning. Such exclusive uses of terms

in language, whether spoken in groups or into mobile phones ensures that if the conversation is overheard it is not understood. That's one of many means of hiding messages in the cryptographic city.

The quote about teenagers is from Augoyard and Torgue's book *Sonic Experience: A Guide to Everyday Sounds*. It makes sense in the context of codes and the city to think about the everyday tactics deployed by ordinary language users to make themselves clear or obscure. Used out of context we might also describe such exchanges as vulgar, common, or even offensive. It is interesting that such banter is associated with the street. We draw on the terminology of urban infrastructure to identify this coded use of language ("street talk," "gutter language") as indexed by the aptly named online *Urban Dictionary* (urbandictionary.com).[21] Some languages and speech patterns have developed specifically to evade comprehension to those outside the circle of interlocutors. For example, Polari developed from slang among actors, circus people, prisoners, and dock workers. It is mostly associated with LGBTQ+ subculture of the 1950s.[22]

Many city features are hidden within code, or at least covert messaging. Navigation provides an obvious example. There's a famous New Yorker cartoon by James Stevenson of a policeman giving directions to a visitor from out of town. The thought balloon above the policeman shows a conventional map, with arrows clearly charting the route to the visitor's destination. That's what this knowledgeable local understands. But the thought balloon above the visitor shows a confused jumble of arbitrary map bits and a tangle of arrows. Navigational instructions require a degree of familiarity to be of use. To encounter a city for the first time is to encounter a series of coded messages. In time, seasoned residents can say, "I understand the code because I've been around it for a decade." These are tacit dimensions of language and social interaction. Under a coded system, what gets communicated is opaque to others in the room. Only the supposed recipient knows what the message is, or that there even is a message.

In these and other ways cities are colonized and formed by layers of messaging intended or customized each for their respective constituencies. But then messages get intercepted, relayed, retranslated, recoded, diverted, and distorted. I see those processes as the general communicative milieu to which cryptography belongs, or perhaps cryptography stands in for the whole communicative enterprise of the city. Before pursuing the ubiquity of cryptography there's more to be said about writing in the city.

Blocks

Any student of urban metaphors will notice the presence of *the block* in the city. There are city blocks. Buildings are made of blocks of stone. Freemasonry trades in the romance of construction with blocks of stone. In the ruins of ancient cities, it is the stone blocks that resist the ravages of time and persist. In imitation of architecture, playful infants make and demolish structures made out of plastic and wooden building blocks. It is well known that the architect Frank Lloyd Wright played with Froebel kindergarten blocks as a child.[23] The 3D virtual platform of the video game Minecraft, at minecraft.net, presents a world made of one-cubic-meter blocks. Even people, animals, and trees are made of blocks in this surprisingly immersive world. As if to illustrate my case for the cryptographic city, among Minecraft's major landmarks is a Masonic Lodge and the imposing neoclassical building known as The Uncensored Library, all made conspicuously of regularly sized blocks.

On the subject of text, graphic artists and page editors will *block* out the general layout of a poster or page with rectangles to indicate where they will place text and pictures, eventually to be printed. Early printing involved blocks of wood with carvings or elements in relief for stamping out patterns with colored inks and dies. Early printing presses used blocks with letters in relief for mass producing texts. We still talk about *blocks of text* as we write, type into a word processor, prepare presentation slides, and lay out pages. A block of text can be moved about while thinking less about the relationships between the block contents and the content of adjacent blocks.

Blocks are portable, at least in the practice and thinking of the designer or planner. More specifically a block is a bounded aggregation that can be treated as a single entity. When using drawing or 3D graphics software I will frequently group elements together so that they can be moved about, as a block.

A block is also an obstruction. A block in the drain is a single entity that needs to be shifted. A roadblock is a collection of people and paraphernalia whose effects on traffic flow are aggregated as a single block. It is the block as a whole that matters and exhibits the required identification and portability for that task and that moment. The block serves as convenient a descriptor of elements, processes, and arrangements in the city as it is in writing.

Spreadsheet City

The process of generating blocks of text is of course *writing*. To produce text is to write. I'm edging in this chapter toward a consideration of writing rather than text. As I will show, writing provides one of the many processes linking the city to cryptography. So, let us move toward *writing*, as an active term.[24]

What does it mean *to write a city*, implied in the title of this chapter? It is worth revisiting the importance of writing in cultural development. Doyen of media studies Marshall McLuhan encouraged digital pioneers with his popular 1960s accounts of how we are under the sway of the technologies of writing and print, and more recently electronic communications. Another scholar Walter Ong (1912–2003), a historian and student of McLuhan, reflected on the influences of technology in culture, not least the way technologies of writing and print have influenced cultural and intellectual developments—that is, the way societies think: their politics and philosophy. He wrote about the influence of bookkeeping and ledgers to be examined further in the context of cryptocurrencies in chapter 7.

Scholars such as Mary Poovey concur and emphasize the development of double-entry bookkeeping in basic commerce such as trading, banking, and lending money.[25] The double-entry aspect refers to keeping two ledgers: one for income, the other for expenditures. These scholars argue that the invention and popularity of double-entry bookkeeping not only aided commerce but also influenced the development of certain intellectual practices, not least, the way we think about order, rationality, and how we present and arrange information, and by implication knowledge.[26] Ubiquitous spreadsheet applications, task lists, schedulers, and online calendars provide contemporary illustrations of how wedded we are in business and personal organization to the tabulation of information.

For Ong, efficient bookkeeping set in train a way of thinking of things in the world as recorded and assigned a monetary value. "The arts and sciences could be viewed as a mass of 'wares,'"[27] he writes, "Here the most diverse products are mingled on an equal footing: wool, wax, incense, coal, iron, and jewels—although they have nothing in common except commercial value."[28] With this kind of calculative assessment, you don't need to look at the wide-ranging qualities of those items: "One has to know only the principles of accounting."[29]

Ong showed that the utility of bookkeeping, ledger writing, provided a benchmark for rationality. The ledger renders transactions transparent, able to be scrutinized, following a calculable logic. The ledger can also be reproduced, as can the procedure, to give the same result. To see the world through the lens of the accountant's ledger is to see a world conveniently divided into transactional components, classified, compared, weighed, evaluated, and eventually balanced.[30] These are further aspects of the city as writing, the city as ledger or spreadsheet, making way for a consideration of city processes that draw on the idea of the blockchain in chapter 7, and hence on cryptography.

Writing the City

You can write *on* a ledger, write *up* a ledger, and even just "write a ledger." Poovey describes the use of the ledger as a "rule-governed writing."[31] I would add that cities are similarly to be written about and written on. Of course, we not only write, but we also read. There is an attractive symmetry in the idea that you might both read and write the city.[32] To write something that isn't text, like a city, gives us pause. It operates figuratively—as a metaphor. To write a city suggests that the city is a book, song, poem, or ledger, or perhaps the second half (the vehicle) of the metaphor is open to whatever the idea of writing suggests to you. So, to write the city might mean to bring it into existence with something like the creative energy that goes into writing a song or a book.

I'm content to think that planners, designers, and citizens are authors who not only write reports and draw diagrams and plans, but who also write our cities. To bring in a performance metaphor, we city dwellers are also improv artists who make it up as we go along. We write and rewrite the script as we move. We write the city as we go about our daily business, all the more now as we (literally) write and read messages on our smartphones on the go, and leave digital traces, like pen strokes, as we negotiate the city.

Some joggers and cyclists carefully calculate routes through the city that result in drawings when viewed on a digital map application.[33] Such "GPS art" writes and inscribes invisible graffiti across the city: dinosaurs, skulls, portraits, logos, names. We write across the city by our movements anyway.

The density of our movements writes like a highlighter pen or sharpie indicating what people value and avoid spatially. Citizens also write over their cities by exerting influence, sometimes unwittingly, through the data they provide or through engagement and direct action via intermediaries such as designers, planners, developers, and decision makers. Citizens as city writers also offer up subversive texts, alternatives, and resistance to city transformations. We also write, annotate, mark up, and inscribe our presence across the city in other secretive ways to be discussed in subsequent chapters.

Writing and drawing are clearly related. The *-graphic* part of the word *cryptographic* makes us think of drawing, but the affix has most to do with writing. The etymonoline.com website describes the common abstract noun ending *-graphy* as a "word-forming element meaning 'process of writing or recording' or 'a writing, recording, or description.'" So, we have geo*graphy*, biblio*graphy*, choreo*graphy*, crypto*graphy*, which primarily write and therefore describe the earth, books, dance, and messages. "To draw" and "to write" are similar in that they can both function as either transitive or intransitive verbs, i.e. they function with or without an object: She draws; she draws a tree; he writes; he writes a book. You can draw just about anything, but in normal usage, writing is more limited. The songwriter Arthur Hamilton exercised simple verb "misuse" with the titles "I Can Sing a Rainbow" and "Cry Me a River." I say "misuse" as that's one of the ways philosophers and poets have characterized metaphor, as a deliberate misclassification: putting rainbows in the same category as songs by suggesting they can be sung, and rivers in the same class as tears and emotions as if the result of sadness or melancholy.

Here is an example of our readiness to think we can write physical objects like cities into existence. The early computer game series *Myst* (1993) played with the grammatical asymmetry of reading and writing. The protagonists had somehow acquired the art of "writing ages," which are islands linked together by specially written link books. The games are populated with 3D models and renderings of tangible spaces, and virtual handwritten books containing descriptions and diagrams of imagined mechanisms and places. Players don't need to look for consistency or logic here. Who would not want to write things into existence with the stroke of a pen! Metaphor and imagination accomplish that for us.

Printing the City

Drawing and writing involve similar processes as long as we think of placing a pen, brush or quill in contact with paper. In the history of technology print supplanted writing by hand as a means of preserving texts. Printing involves a set of procedures that involve reproduction via mechanical processes. How does the transformation from writing to print impact the evolution of cities?

To fill a ledger with numerical data was a particular method of writing. By Ong's account, the invention and adoption of orderly double-entry bookkeeping was among a series of events on the trajectory to modernity. Scholars think of Johannes Gutenberg's (1400–1468) invention of the movable-type printing press as a pivotal moment in the cultural and social development of Europe and beyond. By Marshall McLuhan's reading the printing press ushered in a revolution in thought.[34] Printing firms were able to deploy individual, durable typographic elements (letters and punctuation marks) manufactured in metal and arranged in rows to produce a page of text, the inked imprint of which was transferred to sheets of paper, repeatedly. For McLuhan the industry of movable type was the final triumph of visual over aural culture helping us humans see the physical world as distinct from ourselves, as able to be inventoried, documented, and studied. For McLuhan, the ability to print and distribute multiple copies of texts cheaply and quickly reinforced "homogeneity, uniformity, and continuity"[35] in communication and in culture.

There are other aspects to the technique of movable type. Scholars have considered the Gutenberg revolution in terms of the tools of printing—the characteristics of movable type itself, which after all promoted the utility of modularization and rearrangement. Typographers in printing offices would arrange and rearrange typographic symbols. They could also substitute one symbol for another. Movable type anticipated the intoxicating freedom we have now with on-screen editing, as I move text around, correct, and substitute one symbol, word, phrase line or paragraph for another.

Alberti's Cipher Wheel

The power of moving text across a page predates the printing press. It is worth recalling the earlier innovation of Ramon Llull (1232–1316), the

Catalan polymath who invented the so-called "Ars brevis," "Llullian wheel" or "memory wheel." I first encountered this invention, or at least its representation, as a moment in the lore of artificial intelligence (AI). By the AI account this disk-shaped paper Llullian wheel served as a rudimentary logic machine that worked with combinations and calculations. Scholars are keen to position this device as an early progenitor to the computer.[36] The wheel consisted of a series of concentric disks marked out with godly attributes or "dignities." Historian of cryptography Quinn DuPont identifies the attributes: "goodness, greatness, eternity, power, wisdom, will, virtue, truth, and glory."[37] The wheel would allow a scholar to combine these attributes in various ways to demonstrate the logic of an argument, notably to explain Christian doctrine. According to DuPont: "Each 'dignity' could be combined according to particular rules, which amounted to a method for investigating reality. That is, this method was a way to do work and to actively investigate or 'compute' the world."[38]

Llull's pre-Gutenberg logic machine operated as if ideas can be manipulated, combined, and moved about. The Lullian wheel was also a memory device, a means of recalling and copying the ideal order of the world. According to DuPont, "Lull reconfigured the theory of representation that previously relied on the complex web of resemblances, as it had been handed down to him through ancient and medieval transmission."[39] The *Stanford Encyclopedia*'s entry for Ramon Llull illustrates the wheel, its variants, tables, and complicated and occult nomenclature.[40] Even a cursory glance shows how wedded this kind of rationality is to a mimetic view of the universe, as if representing or imitating higher realities.

Intellectual life pre-Gutenberg appears alien to our current age. For example, Ramon Llull's memory wheel cannot easily be inserted into a linear history in the development of the computer. The device has more in common with secret societies than with computation. A Spanish Freemasonry lodge bears Llull's name. As with the Medieval arts in general, this particular calculative invention confounds attempts to distil any purely utilitarian and computational operations from this occult, mysterious, and cosmological apparatus of reproduction—of divine mimetics. The memory wheel operated in a world imbued with an understanding that art, knowledge, and beauty derived from imitation. The Llullian wheel serves nonetheless as precursor to the cipher wheel, the invention of which is attributed to the influential architect of the Renaissance Leon Battista Alberti (1404–1472).

According to DuPont, "Lull's development of an active system using rotating wheels, with its particular history of representation, was an important precedent for Alberti's invention of the cipher wheel."[41] Alberti's cipher wheel has similarities, but departs from Llull's memory wheel in significant ways, not only in its purpose but also its format. The cipher wheel is more consistent with the combinatorial instrumentality of the Gutenberg revolution.

Gutenberg's printing press allowed for the accurate preservation of texts, contributing to the idea that knowledge accumulates. But there were other benefits as it released energies from the laborious task of copying and transcribing texts by hand and other cumbersome and unreliable processes for reproduction such as woodblock printing. According to social geographer and historian David Lowenthal, "Energies released from tasks of retrieval and preservation could focus on other creative activities, thereby detaching inspiration from the bondage of imitation."[42] So, contrary to Llull, Alberti's cipher wheel, developed under the sway of the printing press and movable type, and signifies a transition to something resembling the modern era. As did Llull's wheel, it adopts the grammar of the sacred circle and axis, and is divided into "houses," as if they are constellations, but it also adopts the new functional processes of mass production: reproduction, modularization, and combination. Like the printing press, Alberti's cipher wheel combines letters of the alphabet. For DuPont, "Both the movable type press and the cipher wheel utilized reproducible, modular, indexical, and combinatory forms of representation."[43]

Alberti's cipher wheel was for cryptographic communication. The technique enabled the transmission of confidential messages between leaders—without the need for interpreters. Alberti wrote, "I can justly consider this cipher worthy of sovereigns, who can use it quite easily, with little effort and without being encumbered by use of an interpreter."[44] Those in communication may be many miles apart even though they share the same language. The interpreter was likely a functionary who would receive a coded message and had the equipment and the knowledge to decode it and pass the translation on to the sovereign. Couriers and interpreters lived dangerous lives, not least for the secrets they knew. Human translators can't easily forget, and easy-to-use translation machines reduced the risk of message leakage from a circuit of human intermediaries.

Alberti Code

I was first alerted to Alberti's cipher wheel in a history display in the Berlin Spy Museum. My own training in architecture had failed to register Alberti's expertise in cryptography. Alberti introduced the cipher wheel in his essay *De componendis cifris* (1466).[45] The cipher wheel is a simple device with an inner and outer disk cut out of bronze sheets (or paper), each marked into twenty-four divisions. The outer disk lays out the letters of the Italian alphabet in upper case and some numbers. The inner disk has lowercase versions of these symbols but in an arbitrary order. The two disks can be rotated freely about the same center. The device provides a simple way of mapping the letters from a text message to create a coded version. As long as the receiver has the same device and knows the alignment of the disks, it is simple to decode the message.

Unfortunately, it's also a simple matter for any codebreaker (cryptanalyst) to work through various letter combinations to come up with a good guess at the correspondences, and eventually the hidden message. Certain letters occur more frequently in any language and that acts as an initial clue for the codebreaker. The clever idea of the cipher wheel is that the coder shifts the alignment of the inner and outer disk at certain points in the message and indicates these shifts to a new alignment by inserting a special character in the coded message. This new mapping effectively scrambles any one-to-one correspondence between a symbol and its coded equivalent, making it harder for codebreakers.

Alberti's cipher wheel looked something like the drawing in figure 2.3, providing a simple equivalence mapping between letters of the alphabet. He used the Latin alphabet, and excluded a few letters as well, perhaps for symmetry. According to a helpful YouTube clip by Ciphertown,[46] the cipher disk user would represent H with two Fs, J with two Is or similar secondary coding. Here's a demonstration of the method. I'll restrict myself to Alberti's character set here to encode the simple communication: WRITE ME A CITY. With the disks in the position shown in figure 2.3 that would result in a simple one-to-one mapping between characters. As long as you know how to align the two disks you could convert my secret message to hmvip &p g lvih. That's actually "VRITE ME A CITV," a necessary variation due to the reduced character set. With the same cipher disk design and alignment,

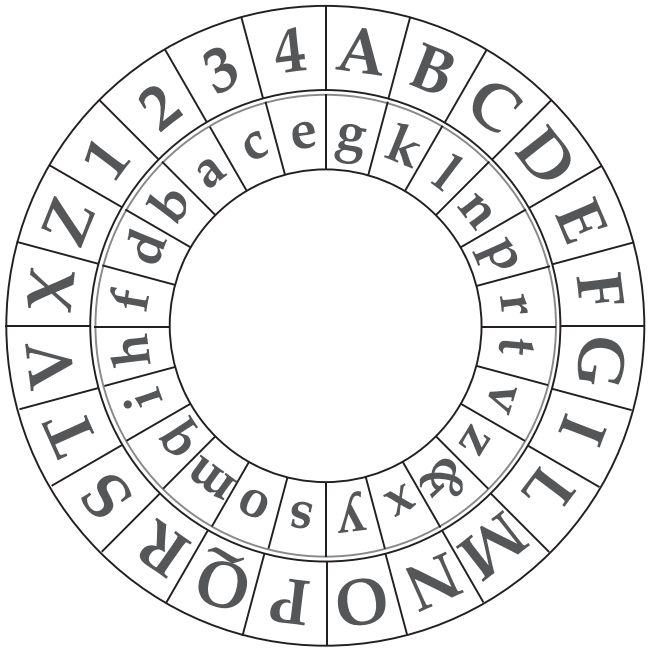


Figure 2.3
Alberti's cipher wheel. Drawn by the author.

the receiver could decode that back to the original message. But that's also relatively easy for an intercepting codebreaker to decipher, even without a similar cipher disk, especially with a longer message, considering letter frequency, something about the context, and iteration through combinations.

Here's another encryption that is more difficult to decode using the same disk design and knowing that the letter g is to serve as an indicator: Ahmvip &p Cc grmq. The appearance of the letter A means align g on the inner disk with A on the outer disk. Taking each letter at a time, when intended message recipients encounter the uppercase letter C they would rotate the inner disk to align g with C to give a different set of mappings (figure 2.4). The coder can insert such rotation cues throughout a long message. That would make it extremely difficult for an intercepting codebreaker to decode the message.

It is a simple process, and there are elaborations on the method to make code breaking even more difficult. Alberti described the shift in alignment as "changing the index", and the family of such methods of shifting the

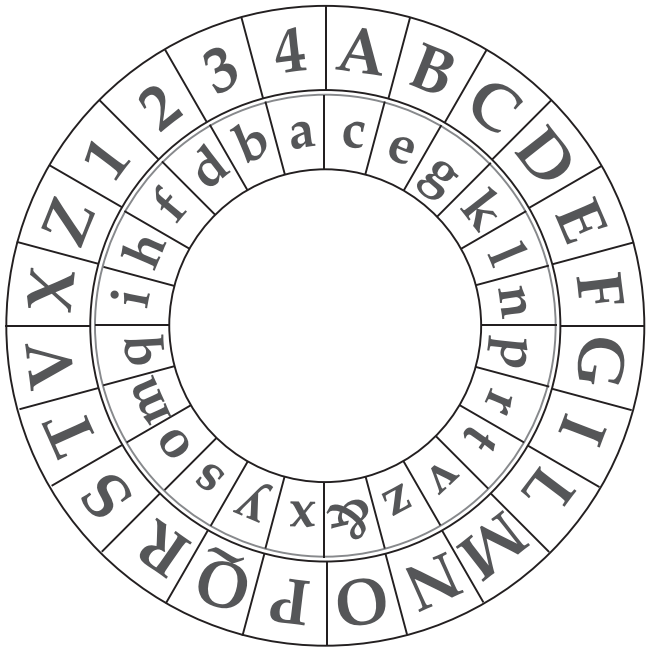


Figure 2.4
Cipher wheel in the rotated position. Drawn by the author.

alphabetical ordering at different points in the message is now called *polyalphabetic encryption*. In *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* Simon Singh provides a helpful history of the cipher wheel's use and elaboration since Alberti.[47] He speculates that such a system could easily have deployed a key in the form of a sequence of letters, perhaps a key word known only to the sender and receiver that would indicate at which letters the alignment of the discs should be adjusted.[48] Though much more elaborate, the German Enigma machine, the electromechanical coding device invented by Arthur Scherbius at the end of World War I, belonged to the same family of encryption machines; this device and method eventually were cracked by the codebreakers of Bletchley Park.[49]

Alberti's interest in mathematics and geometry led him to other coding techniques as well. According to the reading of mathematician and architectural theorist Lionel March, Alberti also projected cabbalist and covert occult methods into the geometry and tiling of the facade for the church of Santa Maria Novella in Florence in such a way that they would

go undetected by church officials.[50] The medium was not of symbols of the kind used in Freemasonry, but "arithmogrammatic 'calculations' to demonstrate theological, particularly christological truths."[51] March identifies Alberti's own name in the coding, as well as "Yahweh." March admits his detailed analysis of the geometry is speculative, but it's fair to say that Alberti's interest in cryptography was integrated into some of his architecture, notably the facade treatment of Santa Maria Novella.

Alberti was in the company of other renaissance polymaths who applied their inventiveness across architecture, sculpture, writing, music, astronomy, and other arts and sciences. That Alberti dabbled in encryption provides just another example of renaissance innovation at work. But by a more interesting reading, Alberti's penchant for encryption is integral to his understanding of architecture. This is the argument advanced by DuPont.[52] It seems that the common factor between architecture and encryption is the influence of the printing press, in other words, movable type, invented and adopted during Alberti's lifetime. Alberti's innovation paralleled radical changes in how people understood language and architecture.

Portable Type

Earlier in this chapter I referred to the portability of text. Portability implies movement, and the dynamic aspects of letters and characters in the printing process as suggesting arrangement and rearrangement. Movable type exerts an influence on architecture and the city. There's a long tradition that considers architecture as the art of arranging things—according to Vitruvius, "the putting of things in their proper places."[53] In his book *Architecture in the Age of Printing*, architectural theorist Mario Carpo maintains that architecture as an art of arrangement reached its apogee with the invention of the movable-type printing press.[54] Alberti was impressed by the idea that letters could be selected and arranged to produce reproducible printed pages. Alberti admitted this influence, and in his book *Art of Building* even used letters of the alphabet to describe the profiles of cornices and moldings. For example, the astragal is shaped "like the letter C surmounted by the letter L."[55] That use of letters hinted at the influence individuated letters had as part of the cultural vocabulary of the time, as metaphors and explanatory devices. It also suggested the "misuse" of letters, a willful obsession with their shape and rearrangement to produce something outside of their usual signifying function, a rudimentary "word art."

Other than this creative digression the architectural tradition of the time seemed to lack a language of innovation. Like the letters of the alphabet, the elements of architecture (columns, walls, roofs, rooms) did not need to be invented, but selected and arranged correctly. There was no appeal then to creation or innovation in the parts. Nor was innovation encouraged in the way elements were to be arranged. In fact, architects were warned against inappropriate placement. Alberti wrote about aberrant forms: "When even the smallest parts of a building are set in their proper place, they add charm; but when positioned somewhere strange, ignoble, or inappropriate, they will be devalued if elegant, ruined if they are anything else."[56] Nature provided the model for perfect arrangements.[57]

By a twenty-first-century interpretation, it's as if Alberti's negative examples harbored the seeds of dissent, if not invention. Aberrant combinations and rule breaking, as in architecture and all the arts, did of course exist in these traditions, but was exercised in the outcast world of the carnival and the trickster.[58] Though *The Art of Building* was saturated with convention and propriety, I'm prepared to concede that Alberti was on the way to thinking of architecture in terms of inventive arrangement and rearrangement. By my reading, that observation aligns architectural innovation with the affordances of the printing press and with media theorists such as Marshall McLuhan.

Leibniz's Secret Machine

The flowering of the intellectual development in Europe known as the Baroque period followed two centuries after the introduction of the movable-type printing press. Chief among the period's luminaries was the mathematician and philosopher Gottfried Leibniz (1646–1716). There are at least three touchpoints connecting Leibniz with cryptography. First, Leibniz invented and built a mechanical calculator. But less well known is his unbuilt model of a machine for encrypting and decrypting messages, using the polyalphabetical encryption method, though with many more moving parts than Alberti's cipher disc. In his account of Leibniz's machines, the philosopher Nicholas Rescher notes: "The calculating machine performs mind-like processes in relation to reasoning, and the cipher machine performs mind-like processes in relation to communication."[59] So, Leibniz aimed to demonstrate by his mechanical inventiveness the two main functions of human cognition as he saw them: *calculation* and *communication*.

Leibniz pitched the cryptographic machine to his emperor, who failed to provide support for the manufacture of a prototype. As Leibniz thought the device was only for princes, according to Rescher, "this apparatus was Leibniz's most closely guarded secret."[60] It was never built, though others (e.g., Nicholas Rescher) have since attempted to replicate it.

Second, much of what we know about Leibniz's life comes from his biographer Johann Georg von Eckhart (1664–1730). Around age twenty, Leibniz spent a year as the secretary of a secret society of alchemists. An article by George Ross probes the claims and counterclaims of Leibniz's commitment to alchemy. Ross provides an interesting excerpt from Eckhart, delivering a tip on how to inveigle your way into a secret society:

> "Now, since he [Leibniz] was curious about everything, he was very keen to have some practice in chemistry as well; so he considered all the various ways of getting access to these secrets. The director of the society was a priest. So he devised the following trick, as he himself often told me with a laugh. He got hold of some very difficult books on chemistry, and noted down the obscurest phraseology he could find in them. Out of these he composed a letter to the priest, which even he himself did not understand, and in it he also requested admission to the secret society. On reading the letter, the priest came to the conclusion that the young Leibniz must be a true adept, and not only gave him access to the laboratory, but asked him to become their assistant and secretary."[61]

Ross is keen to dispel any notion that alchemical mystery cultism had significant impact on Leibniz's mature philosophy, apart from demonstrating his ambition and opportunism. I'm prepared to see this episode as evidence of a philosopher's curiosity. Curiosity draws people to secrets, and even to promote and exploit them. Like many luminaries of this period, Leibniz knew of occult practices, and was even familiar with Gaffarel's writing on "the celestial Hebrew alphabet."[62]

Third, Leibniz famously defined, or redefined the concept of the monad. According to the *Stanford Encyclopedia of Philosophy*, "The ultimate expression of Leibniz's view comes in his celebrated theory of monads, in which the only beings that will count as genuine substances and hence be considered real are mind-like simple substances endowed with perception and appetite."[63] In other words, the world is made up of perceptual units. According to Leibniz's philosophical idealism, monads are the only things that are *real*. Monads are also indivisible. Among the definitions he provides in the essay *Monadology*, Leibniz asserts, "the Monads have no windows, through which anything could come in or go out."[64]

Leibniz's *Monadology* is of interest, especially as inflected through the writing of the twentieth-century philosophers Gilles Deleuze and Felix Guattari, for whom the term *monadology* invokes the notion of *nomad*ology, the study of how sedentary power is permeated by itinerants as if from the outside. The simple formulation of the "windowless" monad operates at least as a provocative metaphor. Through its explanation in terms of spaces and windows, nomadology brings Leibniz's philosophy further into the orbit of architecture and secret places, such as *crypts*. In his book *The Fold: Leibniz and the Baroque*, Gilles Deleuze states, "A 'cryptography' is needed which would both enumerate nature and decipher the soul, see into the coils of matter and read in the folds of the soul."[65] Deleuze elaborates on the metaphor of the fold to explain the art and architecture of the Baroque, a useful subject with which to culminate this chapter on writing, arrangement, and architecture.

Fabrics and Folds

Folds appear in fabrics. What is the fabric in this case? It is a kind of surface, boundary, or border between two places or conditions. Put simply, the fabric to which Deleuze refers is the boundary within the Platonic universe between the world of ideas and the material world: you could say, between the macrocosm and the microcosm; the heavenly and the earthly; or souls and materials. For Plato that would be a boundary between the real but invisible and immutable world of ideals, of which the material earthly world is a pale shadow.[66]

I began to appreciate the significance of the fold in Baroque architecture on a visit to St. Peters Cathedral in Trier, Germany. The cathedral is mostly Romanesque, but behind the main altar the visitor has a view into the Baroque chapel for the relic of the Seamless Robe of Jesus. As illustrated in the Trier chapel, Baroque surfaces do fold, as if affording glimpses between realms. Deleuze provides an account of the Baroque fold that has inspired many speculative architectural and urban design studio projects.[67] Notice Deleuze's reference to levels, compartments, and windows: "There are souls below—animal, open to sensation—or even bottom levels in souls, and the coils of matter surround them, envelop them. When we discover that souls can have no windows to the outside, we will need, at least at first, to think of this in reference to the souls above, the rational souls, which have risen

to the other level ('elevation'). It is the upper level which has no window: a darkened compartment or study, furnished only with a stretched cloth 'diversified by folds,' like the bottom layer of skin exposed."[68]

He supports this description with a crudely drawn cross section through an allegorical building he calls "The Baroque House." There's clearly an upper and lower story, and the folding elements "spiral" into the upper reaches. This is an inverted crypt—there are no windows in the upper story. In this book (*The Fold*), Deleuze references Leibniz's concept of the windowless monad, the indivisible unit of perception, or the "mind-like simple substances endowed with perception and appetite" as explained in the *Stanford Encyclopedia*.[69] These are further reminders of the confluence between architecture and cryptography.

Of even greater relevance to the theme of cryptography, Leibniz was a distinguished mathematician (as well as designer of a cryptographic machine), responsible in part for the invention of calculus, which deals in rates of change, in other words, the slopes of mathematical curves, as well as areas under curves, techniques that will assume greater significance as I probe methods of digital encryption.

In this chapter I examined writing and arranging letters as a simulacrum for arranging city elements (public and private spaces, buildings, parks, roads, street furniture, signage), a process the theories of which are inspired by ordering and reordering letters in a movable type printer. That took me on a journey through Alberti's cipher wheel, one of the earliest systematic and replicable methods for encrypting messages. The technology later developed into sophisticated coding methods such as the polyalphabetic Enigma coding device. Alberti's cipher wheel and his influence in architecture and urbanism entitles architecture to claim a pivotal place in the history and theory of cryptography, and hence as curator of the cryptographic city. I also recruited the rationalism of Leibniz, the Baroque, and Deleuze's provocative spatialization of the monad as progenitors of the cryptographic city idea.

In order to link the spatial *assemblies* or *combinations* of the city with cryptography, we could do well to examine cryptographic puzzles, the subject of chapter 4. In the meantime, if cities are places of reading and writing, they are also sites of coded communication, the subjects of chapter 3.

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in ITC Stone Serif Std and ITC Stone Sans Std by New Best-set Typesetters Ltd.

Library of Congress Cataloging-in-Publication Data

Names: Coyne, Richard, author.
Title: Cryptographic city : decoding the smart metropolis / Richard Coyne.
Description: Cambridge, Massachusetts ; London, England : The MIT Press, [2023] | Includes bibliographical references and index.
Identifiers: LCCN 2022021507 (print) | LCCN 2022021508 (ebook) | ISBN 9780262545679 (paperback) | ISBN 9780262374811 (pdf) | ISBN 9780262374828 (epub)
Subjects: LCSH: Smart cities. | Internet of things. | Urban development—Data processing. | Public administration—Security measures. | Data encryption (Computer science)
Classification: LCC TD159.4 .C69 2023 (print) | LCC TD159.4 (ebook) | DDC 004.67/8—dc23/eng/20221011
LC record available at https://lccn.loc.gov/2022021507
LC ebook record available at https://lccn.loc.gov/2022021508

10 9 8 7 6 5 4 3 2 1