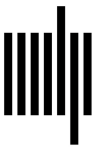
Cryptographic City

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

Introduction: The Urban Cryptographer

In this book I want to bring cryptography into mainstream thinking about cities. Cryptography supports data security and privacy online and serves as a remedy against cybercrime and information leakage. Cryptography also supports cryptocurrencies, the blockchain, non-fungible tokens (NFTs), smart contracts, and other digital innovations that permeate the so-called "smart city." Cryptographic methods and technologies at times appear exotic and external to the concerns of those of us interested in the history, design, and shaping of cities, but in what follows I will demonstrate that cities are already invested in cryptographic ideas and practices. At the very least, cities and cryptography have concepts and procedures in common.

Without cryptography, communications among people and digital devices would be exposed for anyone to see, hack, and misdirect. Facilities for securing transactions are critical elements in city infrastructures. Cryptography applies procedures and algorithms to transform texts, pictures, audio, files, and information flows so they can be read only by a targeted recipient, a designated receiver. Cryptography is not new to the city. As long as cities have existed, communications would circulate, often in full sight, but with their messages hidden. I wish to claim cryptography as a major component in the perennial life of any city.

Formal and informal secret signals, sometimes described simply as "codes," flourish in urban contexts. Think of a knock at the door, the subtle inflection of which is known only to the conspirators, partygoers, or lovers on either side. I think also of how people exchange cryptic text messages, or the coded calls to children and pets that dinner is ready. The urban lifeworld is infused with abstruse acoustic signals that strengthen invisible connections and define spaces.[1] In 2015 an anonymous post on the social

news forum Reddit invited readers to provide examples of codes that only "people in the know" would recognize.[2] "Code black" announced over the public address system tells security staff there may be a bomb in the building. "Inspector Sands to the control room, please" is a call to action for railway station staff in an emergency.[3] Coded signals are also visual. When people used to go door to door asking for handouts, we would hear of so-called "hoboglyphs," chalk marks on fenceposts of suburban houses placed there to inform fellow travelers whether or not the occupant is generous. I once saw someone tipping little piles of white flour on the curbside along my street. Later I discovered that the deposits were waymarkers for an orienteering event, signals meaningful to the runners (Hash House Harriers) who later tramped down the street.[4]

Sometimes secret messages are signs directed to a particular recipient or group. There's a specific audience, and the message is of the moment: "Inspector Sands to the control room." In other cases, the target audience is specific though the timing is not. For example, utilities, inspection points, and street furniture are overlaid with texts, numbers, barcodes, and QR codes that link parts of an infrastructure to inventories and are essential signs for inspectors and technicians who happen across them in the course of their work. Those signs are undecipherable to the rest of us. We don't even notice them. Cities are also littered with remnants of signs meant for the members of a team, but not for us. Some are of historical interest. There's a "v" shape chiseled into one of the stone steps of my tenement block. Next to it is carved the number 14, presumably a remnant of an instruction during the building's construction in the 1830s.

Cities are inscribed with formal markings such as crests, insignias, Latin inscriptions, and symbols, some of which require investigation or instruction to interpret. Their involvement in the realms of cryptography is somewhat accidental; their credentials reside simply in being mysterious to those of us in a different time, place, and culture than their originators.

Not all codes fit within widely sanctioned social norms and well-ordered urban governance. Some obscure messages are delivered as protest or in-jokes concealed within street art and graffiti. Many such purposefully transgressive signals mark territory, and define regions, neighborhoods, and activity zones for particular local communities, groups, and subcultures.

Consumer culture has its own codes and rationales. In advertising, the coding extends to subliminal messaging and other covert signals amplifying

the imperative to conform and consume. Ubiquitous fixed digital-display screens and their handheld surrogates, along with electronic tags and geolocation apps, incorporate many of these cryptographic signaling functions, not least in digital advertising.

Graffiti tags, obscure markings left by a stonemason, and a service code on a fire hydrant are unlikely to serve as vehicles for the delivery of covert messages of the moment: that an invasion is imminent, your Uber has arrived, let's meet for coffee at 15:00. Code experts usually apply the term *cryptography* to deliberately composed covert messaging. In these cases the cryptographic process follows particular methods and procedures and is more instrumental and systematic than I have described so far, as I will elaborate in the course of this book.

Some Cryptographic Terminology

I have mentioned "code" a few times. *Code* is a useful term, not least as it embraces multiple meanings: rules, laws, computer programs, hidden messages.[5] You can code and decode messages, but as we shall see, the terminology around cryptography is more precise. It invokes meanings related to *hidden writing*. I've also referred to messages that are *undecipherable*. According to Simon Singh in *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, "A cipher is the name given to any form of cryptographic substitution in which each letter is replaced by another letter or symbol."[6] The references to "letter" assume a message that appears to human beings in text format. Symbols as discrete shapes and lines corresponding in some way to numbers, characters, and letters of the alphabet can be similarly cryptographic. Filmgoers, readers of detective stories, and gamers probably associate *ciphers* with recreational challenges and mystery stories, such as Dan Brown's *The Lost Symbol* in which we read, "The first character on the pyramid looked like a down arrow or a chalice"—that was "the letter S." [7] The association with mystery stories is reasonable. Cryptography experts commonly apply the term *cipher* to pre-electronic or digital encryption requiring codebooks, procedures, and manually operated devices. The message recipient has at their disposal a means to translate the cipher back to plain text. The *cipher text* is the string of characters produced once the message has been encrypted; the *plain text* is the original message in ordinary language. In his seminal 1960s book *The*

Codebreakers: The Story of Secret Writing, David Kahn describes *cryptology* as "the science that embraces cryptography and cryptanalysis."[8] So it implies a wider field of study than the development of methods. My adoption of "urban cryptology" advocates for such a broad-ranging study in terms of the history, theory, culture, politics, practices, and shared legacies of city development and design.

As hidden writing, *cryptography* applies to a system for translating any message from plain text into a form that obscures the message for everyone except the designated receiver. A *cryptogram* is another term for a message written in this way. You can also refer to such a concealed message as an "encrypted message" or an "encryption." To encrypt and decrypt are to convert a plain text message into a cryptogram and back again. The names given to disciplines that develop and study methods for encrypting and decrypting messages include *cryptography* and *cryptology*.

Adopting some of the terminology of semiotics, a message is a species of *signal*.[9] Signals are messages that are yet to be interpreted by human or other sentient agents. In the digital domain, algorithms check, authenticate, certify, and validate digital signals by means that often involve encryption. Cryptography applies not only to obscuring plain text messages, but also to concealing, protecting, and securing any data, process, protocol, or method of access in such a way as to render it opaque to a majority of human, animal, and machine agents. The idea of substituting letters and symbols to encrypt and transmit a singular plain text message may appear quaint in the current age of ubiquitous, rapid, and multiplied processing of secure digital signals, but the same terminology applies, and throughout this book I will enlist both pre-digital and digital examples to make the case for the cryptographic city.

The *graphic* in *cryptographic* emphasizes writing. To think of cryptography as practices in secret writing, hiding and controlling access, helps my case in asserting the ubiquity of cryptography in the city. As I will examine in chapter 2, writing provides an appropriate metaphor for the generation of meaning in cities.

Some of the examples I have provided so far apply to the visible and external fabric of the city as if cryptographic writing is imprinted onto surfaces. In this book I want to show how cryptography runs deep within the structure of the city. A city is a multilayered repository of covert communications and overlays of texts.

The word *crypto* derives from the ancient Greek word *kruptos* meaning *hidden*. It serves my purpose in describing the cryptographic city to deploy cryptography as the leitmotif for anything that is hidden. Most things in the world are hidden from the senses and the intellect. That hiddenness may be inadvertent, incidental, and even accidental. Lacking capabilities or machines that are omniscient we rely on interpretation to understand our world, and only ever in part.[10] Hiddenness also raises the questions of who things are hidden from and by what means. In many cases the agencies of necessary obscurity include coteries of experts, administrative organizations, bureaucracies and security officials, the walls of which are breached only by elaborate procedures and protocols.[11]

Computer programs, algorithms, and databases are inevitably hidden from human inspection. Programs and data contain values, variables, and processes that are invisible even before they are processed by encryption software. In this sense all digital processing is *cryptic*, and by extension cryptographic. Cities are similarly made up of hidden processes. Cities are also cryptic in so far as they involve forms of writing or are understood through metaphors of writing. I argue in this book that cryptography provides a new and effective lens through which to inspect these aspects of the contemporary city.

Smart Enough Cities

In this book I will use the term *city* broadly to capture the concepts of a dense aggregation of people, activities, and infrastructures. To date, cities are also major sites of innovation. They concentrate developments occurring in suburban, peri-urban, and rural settings and facilitate their dissemination.

Although this book is about the *cryptographic* city, the technologies, claims, and challenges of the so-called *smart* city provide the backdrop to this study.[12] Smart city infrastructures, platforms, and processes deploy apps, sensors, actuators, algorithms, artificial intelligence, and encrypted flows of big data to ease access to urban functionality and ostensibly to keep us safe, informed, and in touch. A smart city uses data sourced from traffic movement, air temperature, sunlight, and myriad scanners and sensors to activate elements of the built environment: adjust traffic lights, open and close access points, activate shading, turn up the heating, direct

flows through grids, and send messages to people, machines, networks, and systems. A smart public transportation network is one where schedules and real-time data are delivered on demand to smartphone users. Such a smart system enables travelers to transition from bus to train to light rail without having to wait for connections. The system adapts its information flows to the travelers' changing needs and circumstances. Effective public transportation participates in what urban geographers Mónica Degen and Gillian Rose describe as "flows of people constantly on the move."[13]

Efficient digital retail is another indicator of a putative smart city. Market competition provides strong incentives for retailers to provide anywhere/anytime browsing, selecting, comparing, delivering, upgrading, maintaining, repairing, and recycling of consumer products. The smart city idea extends such convenience and efficiency to city sanitation, health care, education, and governance, as well as smart grids[14] and consumer monitoring of metered local and citywide water, gas, and power networks.

A smart city ostensibly filters, delivers, and displays information for the convenience of service users and decision makers. Urban critic Shannon Mattern describes a smart-city screen dashboard as "an assemblage of tickers, gauges, feeds, and widgets that register whatever is measurable and trackable within the smart city."[15] Citizens and visitors in the smart city draw on rich infrastructures for communication and exchange via their smartphones and other mobile devices. For Degen and Rose, the smartphone screen is "the interface between the corporeal body and the smart city."[16]

Not only phones, tablets, and desk computers but also everyday products and services connect via the Internet to produce an Internet of Things (IoT). These "things" include "Smart toasters, connected rectal thermometers and fitness collars for dogs"[17] according to a lighthearted summary in *Wired*, with the potential and challenges such connectivity implies.

Smart city infrastructures carry consequences for the form of cities. Consider digital commerce within the smart city. Digital transactions have undoubtedly influenced the form of cities. Online shopping has reconfigured the pattern of retail. Under the influence of digital commerce, new consumer behaviors have brought major physical retail outlets to a close, and spawned others, such as checkout-free grocery stores. Digital commerce has emptied some city streets of activity and introduced new urban retail and leisure practices. Changes in patterns of working from home enabled

by secure digital tools adjust the footprint of offices in the city, altering the supply of desk workers who would otherwise flood into city cafes and bars during time out from work. Working from home has affected office developments and introduced new spaces such as neighborhood-based work hubs, shared working environments, and the redistribution of office support services. City visitors mediate their access to accommodations, attractions, and shops via digital platforms such as Airbnb, which in turn exert pressures that change living patterns and property markets, not to mention supply, delivery, and manufacture further upchain. Add to this digital context self-drive road vehicles and secure drone-delivery infrastructures.[18] Apart from the physical structures of cities, online activity by businesses and consumers alters the way people interact with each other and with systems and services.

Securing the Smart City

None of these smart city innovations would be possible were it not for secure financial transactions, data flows, media streaming, and communications made possible by encryption. In these and other ways, cryptography plays a crucial role in the shaping of cities.

Any highly interlinked networked system is vulnerable to exploitation. The ubiquity of the Internet amplifies the risks to the security of the smart city. After all, the Internet is an open system whose default ethos and operational mode is to "share." Early myths about Internet hackers drew on the idea that anyone could tap into the flow of data to steal and alter it. According to a review article on cybersecurity in smart cities by Armin Alibasic and colleagues, threats have moved on from solitary hackers and opportunists to "highly skilled and organized professionals who are able to deploy a variety of sophisticated techniques to launch complex and coordinated attacks."[19] The researchers list these well-known bad actions as hacking and malware, zero days, botnets, denial of service (DoS), and distributed denial of service (DDoS).[20] The online book the *Cybersecurity Bible* by Hugo Hoffman presents a sobering compendium of such risks.

Cybersecurity challenges are further inflected by large centralized data hubs, the cloud, and so-called "edge computing"[21] where heavy-duty processing occurs at the site where it is needed rather than ported over the Internet. Each method introduces its own vulnerabilities.

Wireless communication adds further challenges in what one cybersecurity firm describes as the "huge and unknown attack surface on smarter cities."[22] The security firm lists targets for such urban surface vulnerabilities as traffic control, street lighting, city management, sensor arrays, public data, mobile applications, cloud and software services, smart grids, public transportation, surveillance cameras, social media, and location-based services. They show that "hacking wireless sensors is an easy way to remotely launch cyber-attacks over a city's critical infrastructure."[23] Among the vulnerabilities in each of these systems they illustrate how hackers can feed false data to exploit wireless sensor technologies and cause disruption. They provide several graphic examples: "Attackers could even fake an earthquake, tunnel, or bridge breakage, flood, gun shooting, and so on, raising alarms and causing general panic."[24] They even posit the channeling of fake data from smell or rubbish sensors causing garbage collectors to clog the streets at critical times. Cyberattacks are technical vulnerabilities that have functional, social, economic, political, and cultural effects.[25]

Smart City Narratives

By now it will be apparent that I'm moving from *smart* to *cryptographic* as the moniker of the contemporary city. But the "smart city" idea captures enthusiasms for technological innovations, many yet to be realized. The smart city also presents as a cultural *aspiration* that propels planners, policy makers, service providers and citizens toward putatively rational "data-driven" decision-making. Urban critic Shannon Mattern describes this emphasis on "whatever is measurable and trackable within the smart city" as revealing an "instrumental logic."[26] The smart city is a way of talking about the city and its challenges that adopts a certain technological gravitas. It is a formative construct in narratives about the city.[27]

The idea of the smart city is not new, though it was a concept formerly described in terms of *intelligence*. In a 1980s book entitled *Teleports and the Intelligent City*, Andrew Lipman and colleagues argued that the intelligent city would be shaped by "abundant computer-literate workers," the spread of telecommunications, "the diffusion of the personal computer in households," and "acceptance of automated decision support systems (e.g., artificial intelligence and 'expert' systems)."[28] Admittedly, the smart city

avoids some of the overly ambitious and threatening connotations of artificial intelligence.

The smart city comes across as a catch-all for a portfolio of ambitions and initiatives. It serves in branding campaigns, and as a way of attracting businesses, developers, and a workforce to a city. It carries the helpful ambiguity that the smartness may apply to the citizens, its workforce, governance, or its technology. It also carries aesthetic connotations of spatial neatness, order, and style.[29]

Rival discourses and metaphors compete with smart city advocacy. The "sustainable city" is another category of city narrative.[30] Concerns about biodiversity, climate justice, and water poverty are addressed in the sustainable city literature, but rarely problematized or addressed through the lens of the smart city. Smart city advocacy easily assumes that digital technology has the capacity to address sustainability and other urban challenges if not now, then in the future. In her arguments against the rhetoric of the smart city, Mattern declares that she's "annoyed by its elasticity, ubiquity, and deceptiveness—and its sullying association with real estate development, 'technosolutionism,' and neoliberalism."[31]

Encrypted security measures are a key response to the vulnerabilities of the smart city. The practical matter of security and the productive links to urban semiotics led me to favor the term *cryptographic city* in place of *smart city* throughout this book—or at least to test the limits of a cryptographic framing of the urban condition.

Crypto-skepticism

Cryptography can also present in a negative light. It is easy to think of encryption as a necessary vice that locks cities down, rendering them impervious, constrained by esoteric security protocols. In so far as cryptography translates plain text into something less readable, it denies the richness of language and communication.

An encrypted signal gains and delivers nothing by its circulation. It acquires no nuance, accretes no new meanings. It is meant to be incomprehensible anyway, except to a designated recipient, and bypass those communities, cultures, and influences that lie between the originator and the targeted recipient. Encryption reinforces an exclusive and elite relationship

between sender and receiver, subjecting others to the noise of unreadable signals. The automated translation of a plain text message into a secret code and back again involves little human interpretative capability. Translating a text message into and out of its encrypted format is procedural and algorithmic.

We might therefore think of cryptography as devoid of humanity. A message gets translated into code, which is then unpacked by an agent receiving it and according to an algorithm. There is no scope for nuance or interpretation in the process. For critics, contemporary digital encryption epitomizes the restrictive, mechanistic, dehumanized, and inauthentic commerce that is digital communication.

The word *cipher* is the Arabic and Old French word for *zero*, also defining a person of no significance. Carl Jung wrote, "If . . . I despise myself as merely a statistical cipher, my life has no meaning and is not worth living."[32] By *statistical cipher* he meant the human being turned into a number. That is a common trope characterising the targets of statistical aggregation, bureaucracy, militarism, consumerism, and confinement. In this light, cryptography as writing in cipher is yet another example of this reduction of our humanity.

Cryptography also signals social failure, demonstrating mistrust. For critic Shoshana Zuboff encryption is an admission of defeat in the face of a pervasive lack of trust in the organizations, technologies, and state instruments that manage our data. She writes about how digital platforms harvest and exploit our personal data. As data is being drained unceasingly from our interactions with one another we find that encryption is the only recourse left "when we sit around the dinner table and casually ponder how to hide from the forces that hide from us."[33] She's referring to the way social media platforms harvest our personal data and sell it to others. The only way to protect ourselves is to make our communications incomprehensible to those who would exploit it. Cryptography underscores mistrust, even as it seeks to alleviate it.

A focus on cryptography also heightens other anxieties. A practical book by cryptography and cybersecurity researcher Keith Martin bears the title *Cryptography: The Key to Digital Security, How It Works, and Why It Matters*.[34] He alerts us to the pitfalls of not taking cryptography seriously: "If you are inadvertently too trusting when opening an unsolicited link to an amusing video of a dancing sheep, then your computer could easily be inducted into a global network of machines conducting criminal activities. Your

computer might end up attacking mine."[35] Such concerns present as an undercurrent of anxiety to our otherwise unfettered use of networked communications. I will leave it to security advocates to elaborate such warnings and exhort computer users to engage more with the topic and to exercise increased care.

Though I am intrigued by the subject, I recognize that not everyone is fascinated by the allure of code. Cryptography can be highly technical and mathematical and is a topic many are willing to leave to the experts. We might have to attend to cryptography when reminded to choose a more secure password, and to be cautious when disclosing information about ourselves, and when parting with money. But we don't need to know its methods to do so. As with any technical study, cryptography as a topic is subject to the vagaries of taste as much as knowledge and competence.

In a helpful book on the history and legacies of cryptography, Katherine Ellison defends cryptography against some of the charges I've outlined. She agrees: "A cipher must be precise, and it must follow rules agreed upon by correspondents."[36] But in answer to the crypto-skeptics, she argues that the history of cryptography is woven into the history of emotion, and calamity, it's the last desperate resort in addressing or expressing "loss or impending death, defeat, and struggle."[37] The art and practice of cryptography also demonstrates that "ambiguity, imprecision, and flexibility characterize human language even when it is ciphered."[38] From a historical perspective she shows that skills in the art of cryptography are human and fallible: "Cipherers and decipherers do make mistakes."[39] She maintains that the stories of these imperfections can inform cultural history. She reminds us of the rich language practices that contribute to the message that is to be encrypted and the meanings and actions that it may invoke in the recipient: "Communication in cipher also requires communication not in cipher, before the cipher, when the rules are put in place and shared, when the message is decided upon. And this communication, in turn, is passed on orally or, in the case of the cryptography manuals, in print."[40]

Something similar applies in the case of telephone and video communication. Electrical impulses and binary signals between sender and receiver pick up no nuance along the way. However, the technological system is at the service of the human agency at either end of the communication channel, which has the potential to participate in the full richness of human language and sociability.

As further illustration of the cultural values evident in cryptographic practices, writers on cryptography throughout history provide awkward and deviant examples. For Ellison, "humor and playfulness characterize the history of cryptography just as much as the drive toward perfection."[41] The study and history of encryption in any case is not always serious. I surmise from her arguments that cryptography is as old as literacy. As a semiotic practice it is hardcoded into the idea of language. In her study of early cryptography manuals, she observes that "the interpretive complexities of both rhetorical and metaphorical language and of language as always coded, and knowledge of the ways in which human languages can and cannot express experience, are central to ciphering and deciphering."[42] Another way of affirming the cultural value of encryption is to observe that ciphers are as old as secrets, which society could not function without.

Cryptography is also at home within the human propensity to identify and solve puzzles. To decrypt an encrypted message without the benefit of a manual or key constitutes a puzzle. It requires that a human codebreaker work quickly and efficiently through a series of combinations. That's a further link between the city and cryptography. Cities are sometimes like puzzles that visitors and residents must "solve" as they go about their business, such as navigating from home to the shops and back. Cities are also spatial arrangements of elements (zones, parks, buildings, neighborhoods), the design of which constitutes an open-ended puzzle for designers, architects, planners, and engaged citizens. In fact, the challenge of cryptography in the city is less a problem of coding and hiding as decoding and exposing. *Accessibility* is the watchword of contemporary, culturally informed urbanism: laying bare rather than hiding things away.

The Accidental Codebreaker

Cryptography conceals and then reveals a signal to the designated receiver. To decrypt or decode is to unhide. Cryptanalysis is the difficult process of uncovering a secret message without the entitlements of the intended recipient, and without a codebook or key. Cryptanalysis is a form of breaking and entering, and often referred to as *codebreaking*. Stories of the World War II decoders at Bletchley Park focus less on the clever methods employed by the Germans to encode messages to U-boats.[43] It is the various means by which the Allied codebreakers (cryptanalysts) cracked the code, and their

methods for sustaining that subterfuge, that captures the imagination. The invention of a secure coding system involves a substantial intellectual effort. But once created, it takes more intellectual and material resources to break the code than to implement it.

Codebreaking applies the endemic human propensity to enjoy and expose secrets. Codebreaking drives the human condition, more so than hiding information. It is the main ingredient of scandal and gossip, which historian Yuval Harari argues has helped homo sapiens maintain their sense of community.[44] Gossip is a way of sharing intelligence and of bonding. By our natures we seek out, as detectives and forensic scientists.[45] The prevalence of conspiracy theories provides further evidence for the priority of forensic-style interpretation. Even when there's nothing to find, we keep looking, like conspiracy theorists convinced of extraterrestrials or stolen election ballots.[46] The search, breaking the code, is sustained within the shared imaginations of communities, however fevered. Whether by intention, habitual storytelling, or accident, we are codebreakers, a human faculty that assumes even greater importance as we think of urban environments as already "coded."

Urban Affordances

Encrypted communication systems and cryptographic methods *afford* certain opportunities and risks for the city. Throughout this book I will draw on the concept of *affordance,* so it warrants some explanation at the outset. The term *affordance* was adopted by the psychologist James J. Gibson (1904–1997): "The affordances of the environment are what it offers the animal, what it provides or furnishes, either for good or ill."[47] He introduced the concept by referring to the relationship between the nonhuman animal (water bugs and bears) and its environment, though he and others also developed the concepts in the relationship between people and designed artifacts.[48] Affordances are properties of an object that present themselves as we interact with it. The doorway in a building provides an obvious example. A surveyor might measure the doorway in terms of its dimensions. But an assessment of the affordance of the doorway depends on who might use it. For someone with full mobility the doorway affords convenient passage from one space to another in the building, for someone in a wheelchair it may afford an impediment to movement, especially if there's a step, the

doorway is narrow, or the door swings toward the traveler. Gibson affirms: "As an affordance of support for a species of animal, however, they have to be measured relative to the animal. They are unique for that animal. They are not just abstract physical properties. They have unity relative to the posture and behavior of the animal being considered. So an affordance cannot be measured as we measure in physics."[49] Other terms come to mind such as *properties* and *qualities*, but properties are abstract, and qualities imply a value judgment. Affordances are situated. To describe the world in terms of affordances puts the focus on experience.

The concept of affordance is relevant in the digital domain, in particular in user experience (UX) design.[50] Designers might speak of the affordance of a dialogue box on the screen for entering a password, the buttons on a smartphone, an emoji, or indeed a whole software package, platform, or service. Concepts and framings also carry affordances. In subsequent chapters I will demonstrate the relationships between affordance, encoding, and encryption.

Urban Cryptography

The chapters that follow will examine city life through the frame of cryptography. Here are some of the affordances of framing the city through an "urban cryptography." The first and most obvious affordance is that cryptography addresses challenges of hiding and securing data and information flows in the city. People, objects, and information hide in cities. By inspecting the city through the lens of cryptography, we understand better the hidden aspects of city life and form. In this case cryptography provides the urban scholar with a pretext for talking about urban hiddenness. A second affordance is that cryptography controls access. The urban challenge of cryptography is to decode and expose rather than secrete its operations within code. Contemporary urbanism celebrates accessibility, which is to lay bare and reveal to all rather than to hide and conceal. Third, cryptography exploits and relies on the properties of profligate combinations. Cryptographic processes mirror and inform what happens in the design, management, and use of city elements and spaces. In his book *The Culture of Cities*, Lewis Mumford identified cities as places where "the goods of civilization are multiplied and manifolded."[51] Cities are also places where combinations of elements, spaces, places, buildings, and infrastructure are

enumerated and tested. I discuss these and other affordances in the rest of this book.

There is a strong linguistic thread to this discussion. Cities rely on and perpetuate sign systems (semiotics). As a branch of semiotics, cryptography develops further the city's place in an economy of signs. In the course of this investigation I will also deploy some of the strategies of design methods and systems theory by recasting them as tactics in cryptography. As an example, rather than dismissing the idea of design as puzzle solving I place it in a more pragmatic light, casting the designer as urban cryptographer.[52]

I will expand on the cultural aspects of cryptography in the chapters grouped into four sections. The first makes a case for an urban cryptography and emphasizes cultures of writing. The second introduces the combinatorial aspects of making, writing, and reading the city. The third delves into algorithms and calculations. The fourth and final section progresses through some extreme ventures that position the cryptographic city in temporal, global, microscopic, and extraterrestrial contexts.

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