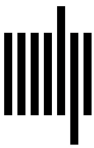
Cryptographic City

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

6 The Dissimulated City

Navigating the city presents as a puzzle for many, at least for the first-time visitor. In this respect the cryptographic city is a game space. Many board-games and video games present cities by way of a simulation. Monopoly offers a minimalist rectilinear abstraction of city streets. The early versions of the video game SimCity showed a city laid out on an isometric grid. A simulation of a building is a model of a building as a physical or digital representation created with a computer modeling program or a scan of an actual building (figure 6.1).

Consider the related word *dissimulation*. A dissimulated city is a city that is not as it appears, and in fact conceals what it is. It is in disguise. It offers a fake or feigned appearance. Cities are multilayered, as if wearing a multitude of disguises. Cities typically support a range of communities, each with its own identity. Any community may allege that others are covering over their particular understanding of the city. For the urban critic there is no end to the process of unmasking layers of disguise. In his influential book *Simulacra and Simulation*, the critic Jean Baudrillard pronounced that so many commercial images "dissimulate the fact that there is nothing behind them,"[1] that there is nothing behind the disguise.

Cities, politics, and systems of justice can dissimulate, disguise, and conceal. As well as political critique, the idea of dissimulation informs the functioning of games. Roger Caillois's seminal book *Man, Play and Games* highlights simulation as a key aspect of play, where a person "forgets, disguises, or temporarily sheds his personality in order to feign another,"[2] and enters a "dissimulation of reality and the substitution of a second reality."[3] Dissimulation is a significant aspect of entertainment, games, puzzles, and the cryptographic city.

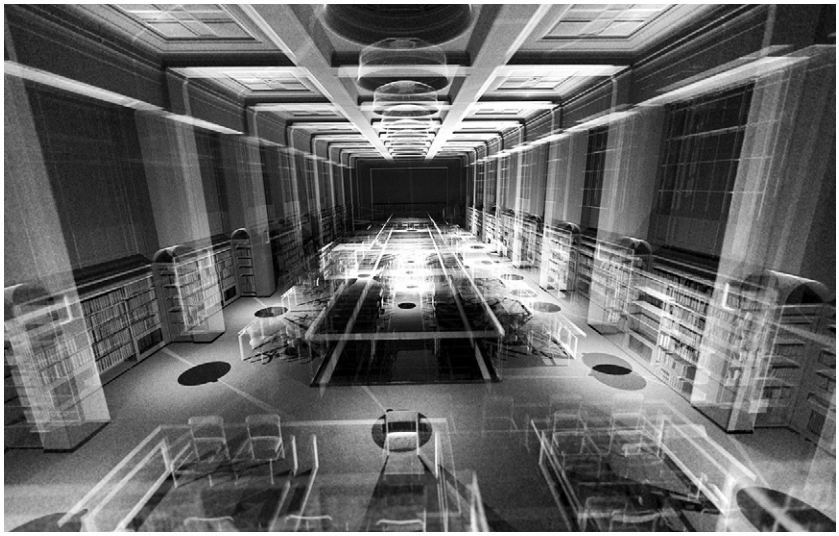


Figure 6.1
An example of 3D dissimulation. LiDAR scan of the National Library of Scotland Reading Room. *Source:* Asad Khan, www.theentropyproject.com.

Dissimulation is a key aspect of encryption. An encryption is a disguise. Consider a simple word puzzle: "I am an urban anarxhist." What am I? The solution is to recognise the errant "x" and replace it with the letter "c" to disclose "I am an urban anarchist." The trivial challenge in this case is to detect that something has been substituted, concealed, or *dissimulated*, disguising an original message. The challenge of decryption is to uncover that original plain text message. Cryptograms are therefore a species of dissimulation: in other words, disguised messages.

The most cunning methods of disguise are those that conceal that a message is in disguise. Ingenious cryptograms conceal to those outside of the communication network that there is even a message in play. I will return to that form of dissimulation in chapter 9.

I want to start in this chapter with the other extreme, where the game elements of the cryptographic city are made conspicuous and are even amplified. Urban *gamification* demonstrates the convergence between digital gaming and the city. This discussion also lays some groundwork for an examination of puzzle solving in cryptography.

Urban Gamification

Gamification involves a range of tactics by which designers encourage reluctant users to adopt novel, unfamiliar, and challenging digital systems and devices. Designers and developers producing human-oriented systems emphasize user experience (UX) design.[4] Citywide UX design comes to the fore with energy-use metering in homes, curbside bike and car rental schemes, accommodation booking, and the panoply of consumer-oriented e-commerce. Contact-tracing apps on smartphones for monitoring and mitigating the spread of infections provide similar UX challenges. Apps for a broad market need to accommodate diverse categories of users, overcome user resistance, and ensure that personal information is secure. There are public and commercial incentives for designers to develop, test, and adapt effective UX design and deploy gamification tactics.

Many of the incentives to lure users into online products and services occur in a competitive commercial environment. Gamification comes across as a commercially motivated tactic for engaging users. It attempts to turn human-computer interaction into a compelling and even addictive experience.[5] By a critical reading, gamification dissimulates the commercial nature of an application, providing a further step toward the commodification of everyday life, reducing urban experience into monetary value or a score, paying little regard to context or diversity of values, and promoting questionable notions of "social credit" ratings.[6] The *Black Mirror* TV program episode titled "Nose Dive" (dir. Joe Wright, 2016) presents a dystopian scenario in which people award one another credit points depending on how they interact with each other, a potent illustration of the dark side of widespread gamification.

Play and Oppression

Life is a game, according to the designation "man the player," *homo ludens*, a term elucidated by the historian Johan Huizinga.[7] The concept of gamification refers to only a part of what being *homo ludens* entails. Even through the limiting lens of instrumentalized, commercialized, and manipulative gamification, the elements of competition, rewards, progression markers, leaderboards, and scores pervade human social organization in urban and

work contexts. Formal education relies on gamification as it grades student work and awards degrees. Management structures award pay grades, job titles, and preferred roles on the basis of performance and loyalty. In democracies, people vote for candidates, and are polled, to produce popularity leaderboards. The motivational aspects of scores, rewards, and leaderboards are palpable among spectators and players at sports events, quiz nights, and management retreats.

The movie *The Circle* (dir. James Ponsoldt, 2015) parodies high-tech companies that provide a putatively pleasant, home-like, and leisurely work environment. Such highly successful companies attempt to develop an *esprit de corps* and encourage internal innovation. The movie includes a sequence where the new desk worker handling customer inquiries is introduced to a method for improving customer satisfaction scores. The play context of the work environment is vital for success in the firm. Workers are also required to participate in weekend social events, and to do so voluntarily. Everything the worker does is logged via social media and rated, so managers and teammates know what you are doing, even after work hours.[8] The drama of the movie revolves around the idea that this is all a dissimulation. The jobs are very insecure. The environment is highly competitive and intrusive and will not tolerate criticism from within. Scores, rewards, leaderboards, and teamwork turn out to be a means of exploiting employees and the audience for the company's social media products.

We don't need to concur that ludic, competitive game elements provide the primary motivation for people to do what they do. An article by game expert Scott Nicholson notes that "players engage with games for an exploration of narrative, to make interesting decisions, and to play with other people."[9] He advocates for "meaningful gamification"[10] that encourages players to explore and develop their own individualized goals and motivations.

We could make similar points about education as a gamified experience. Students don't just seek higher grades in their education, but the challenge of the learning experience, the sociability of university life, or the opportunities afforded after graduation. People in work don't just seek higher pay grades, but fresh challenges, and more interesting interactions. Voters in a political race are not motivated to only see their candidate score higher but expect them to bring about some kind of beneficial change when elected.

Combination as Play

In chapter 5 I explored urban combinatorial complexity. To what extent is gamification an exercise in combinations? The answer to that question will advance my case for the cryptographic city. Combinatorial complexity implicates two of Caillois's other characteristics of the game, as described in *Man, Play and Games*. These are the elements of *contest* and *chance*.

Riddles are combinatorial games. I described some riddles in chapter 4. A riddle is a species of game. It is also an exercise in combining elements: a question often delivered in terms of elements permuted in different ways: "What is greater than God, more evil than the devil, the poor have it, the rich need it, and if you eat it you will die?"[11] The unknown entity x is permuted through a selection of phrases "greater than" and "less than" as well as needs and consequences. The answer is "nothing," though the recipient of the riddle and the answer may have expected a more obvious combinatorial variant: "What is less than God, better than the devil, the poor don't have it, the rich don't need it, and to eat it is to live?" That's part of the challenge of the original riddle. The combination doesn't seem quite right.

A multiple-choice quiz is also an exercise in combinatorial complexity. As known to anyone who has tried to score well in such a quiz, you are competing against the power of combinatorial complexity. With ten questions, each offering four alternative answers (a, b, c, or d), there are over one million combinations of responses. There's about a 1 in 500,000 chance of getting half the questions right by answering randomly, in other words, of passing the test if you are only guessing at the answers. A leaderboard is also an exercise in combinations, displaying participants in different orders. Few of us are able to grasp instinctively the scale of combinatorial tasks. But players want to see their team at the top of the list, and they want to know the ordering; in other words, which of the many orderings is the outcome. The very large number of possible orderings makes the game result unpredictable and helps contestants engage in the process. Team configurations interest players as well. There are over ten million ways of assigning fifty players into five groups of ten. So, choosing which group to join similarly engages you in a contest of combinations.

These play elements pervade the cryptographic city, especially if we think of the increasingly gamified elements of urban amenities and services. They

also facilitate the operations of cryptography. These are key elements in the arrangement of cities, life in the city, and the city's security systems. The discussion so far prepares us to consider the gaming element of cryptography that involves combinations and puzzles.

Keys and Puzzles

I explained encryption keys in chapter 3. Someone trying to open your four-digit mechanical combination lock would have to try on average 5,000 combinations (10,400/2). That's about two to five hours of work. Computers perform millions of mathematical operations per second. But some sequences of operations still take a long time, measured in minutes, hours, days, or even years. A computer iterating through a potential eight-character password, sequence of passwords, or encryption key by brute force could take several hours. Security software could detect that someone is repeatedly trying different combinations and would shut them out.

One of the ways to foil hackers is to ensure that the effort in working through combinations to break into a system is not worth it. Deploying a central processing unit (CPU) to search through combinations costs time and resources. You need the hardware, network connectivity, power, and time to do the hack before detection, and hackers may need to work on many accounts or passwords at once. A digital database of financial transactions is a common hacking target. In an unprotected financial database hackers could install false transactions that funnel money to their own accounts. Even a legal account holder might try to adjust transactions in their own account. Banks and other custodians of such financial ledgers deploy increasingly sophisticated cryptographic systems to prevent this doctoring of transactions.

As I will examine in chapter 7, in the case of cryptocurrencies (e.g., Bitcoin) there is no centralized data management. The entire ledger of transactions is farmed out to a widely distributed set of computers in the network, with names and other details encrypted so that you can only read details of your own transactions. The security challenge with such a shared ledger is that anyone (a hacker, attacker, or even a regular customer) could plant false transactions. The method for avoiding this is to make the ledger hard to hack, meaning that the codebreaker would have to expend so much CPU resource that it is either impossible or just not worth the effort.

One of the means of making it difficult to effect changes to a distributed database is to set up an arbitrary computational puzzle. A computer involved in verifying legitimate transactions on the ledger would have to solve a combinatorial puzzle that requires an exorbitant amount of processing power. Finding the solution to the computational puzzle draws on CPU time and energy before the solution to the puzzle is stored with the data you are protecting. As transactions are added to the ledger, they get more and more difficult to unpick. Older transactions become increasingly "immutable," practically impossible to change. A hacker would have to expend much more CPU effort than legitimate users to make alterations. The security method is known as "proof of work" to be explained further in the next chapter.

In this chapter I have emphasized the ubiquity of play, cryptography as play and puzzle solving, and hinted at the central role of the puzzle in securing digital transactions. Newer, more powerful computational processors will allow even faster processing speeds. The benefits this will bring include faster iterations through combinations and permutations. That also implies quicker codebreaking, infiltration of security systems, and hacking. In chapter 14 I'll consider the field of quantum computing, which addresses such challenges, with the perennial demand that security systems are designed to be "future proof."[12]

Cryptographic Commons

I have referred already to encryption as a puzzle or game, evident in the history of encryption and encryption manuals published as recreational reading.[13] Encryption and cryptanalysis are hobbies and pastimes for some, evidenced by the high number of explanatory blogs and YouTube clips on the subject. The arts of cryptography appear in stories and films. Even if we lack the patience to solve such puzzles, many audiences enjoy watching other people wrestle with the challenges of encrypting and codebreaking.

Play is sociable. Players compete with other players. They also collaborate with other players in teams, and there are audiences and spectators to cheer on the protagonists. Even solitary play invites spectators, comparisons with other players, commentary, and sociable discussion. By some lights play serves as a means of defusing more perilous antagonism and social disorder. Teams also function to develop and share skills in the game,

engender trust, and preserve secret tactics, best moves, and vulnerabilities in the opposition.

As I outlined in the introduction to this book, digital cryptography often attracts the charge that it is an impersonal, instrumental, and rigid process devoid of sentiment or human values. To admit digital cryptography into the realms of human sensibility, some researchers develop cryptographic scenarios that claim to amplify more human-centered and social aspects of cryptography and of keeping secrets. I draw the following example from dyne.org that presents itself as a "non-profit free software foundry."

Consider a fictional cryptographic scenario. A spy (intelligence agent) tells a confidant: "If something bad happens to me then contact Colonel Rodgers at the embassy. He'll know what to do." If the confidant is trustworthy then he or she is equipped to carry out the action as needed. But if some misfortune befalls the confidant then the message is lost. An enemy may coerce or torture the confidant to reveal the secret message. One solution is for the spy to tell several people the secret message. But that increases the risk of betrayal or careless disclosure of the secret message. Another solution is to deliver different parts of the message to a number of people, none of whom has the complete message. On the spy's demise the confidants come together and resolve the puzzle of the message. Had the spy given each member of her trusted circle of friends a fragment of a torn-up letter, or a map, then that would have achieved a similar end as the group came together.[14] The full message is revealed when the pieces come together. That's a familiar mystery story trope: the fragments of a talisman are assembled eventually to become a key to open a secret door to a treasure, or different people bring together fragments of a treasure map. In his novel *The Lost Symbol*, Dan Brown helpfully explains, "Long before talisman had magical connotation, it had another meaning 'completion.' From the Greek *telesma*, meaning 'complete,' a talisman was any object or idea that completed another and made it whole."[15]

Consider the map as talisman scenario but with software—the scenario I described in which people bring together the components of a message in case of a crisis. An application demo at secrets.dyne.org/share provides an interesting model for shared complicity in delivering secret messages. The site contains instructions and a single-entry field. You type a few sentences into the field. For example: "If something bad happens to me then contact Colonel Rodgers at the embassy. He'll know what to do." The program then

returns five strings of characters (secrets). These are in code and look like random sequences of characters. The idea is that you email or text-message these five secrets to five of your trusted friends. As the secret is opaque to those friends or anyone else it is not a high-security item. The secret doesn't need to be hidden or invisible. On some signal or other these friends come together. The five secrets serve as a key to unlock your original message. In fact, the entire message is in the secrets. There's nothing stored in a database. The encoding is such that only three of the secrets are required to unlock the message.

The method works even if one or two of the spy's friends are not available to reconstruct the message, or may have lost their secret, or missed the call to action. There's a web page at dyne.org to "combine secrets." Three of your friends paste their string of code in the fields and the message appears intact and in plain text. Only three out of the five friends have to show up to restore the original plain text message, but if even one alphanumeric character out of the three secrets is misplaced, then the message will not be reconstructed. The dyne.org website explains the application of the method: "Secrets can be used to split a secret text into shares to be distributed to friends. When all friends agree, the shares can be combined to retrieve the original secret text, for instance to give consensual access to a lost pin, a password, a list of passwords, a private document or a key to an encrypted volume."[16]

As explained in a 1979 article on this encryption-sharing method,[17] it could be used for authorizing a group decision where the majority is to prevail; for example, more than half the members on a board have to agree before attaching a digital signature to a check. Imagine such a process used in a judicial system, as when an urban planning board has to adjudicate on whether a development is to go ahead, or a planning subcommittee is to release funds for setting up an inquiry. Such applications would fit within overall e-governance strategies for the city.[18]

Though such innovations are delivered through digital technology they present arguably shared, human-centered, sociable approaches to trust. That cryptography can take advantage of trust among groups of agents, human and digitally mediated, resonates with the cooperative aspects of city life and governance. It also suggests applications of digital cryptography that distribute responsibilities for data security.

This chapter began with the idea of simulation, a game function that puts the focus on dissimulation or disguise. I then considered the pros and

cons of gamification, a series of tactics for adopting elements of play in delivering practical, functional computer programs and systems. Contest and chance are major elements in play that relate directly to cryptography. They establish extremely difficult puzzles as a way of securing data and confounding would-be codebreakers. Play also has a sociable aspect, an element that some cryptography experts have sought to reintroduce as a means of securing data flows within a community context. Such procedures stand as an aspiration and a motif of the potential for shared participation in digital security. In the next chapter, I deal with the technologies behind cryptocurrencies, which puts the spotlight on the so-called sharing economy, a further aspiration to support sociability in the cryptographic city.

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