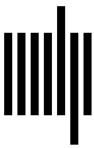
Cryptographic City

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

4 Urban Multiplicity

In his classic book *The Culture of Cities*, published in 1938, Lewis Mumford observed that cities are places where "the goods of civilization are multiplied and manifolded."[1] Cities benefit from mass concentrations of markets and the means of production. In so far as it involves physical spaces, the cryptographic city is a site of intricate combinations, permutations, and arrangements of a multiplicity of zones, buildings, rooms, streets, plazas, gardens, grids, signs, and other infrastructural elements. Combinations compound the challenges of multiplicity. The greater the number of books in my bookcase, the larger the number of ways they can be arranged: by size, color, author, title, and randomly. There are over three million alternative orderings of just ten books on a shelf.[2] Any spatial arrangement—including the organization of apartments in a multistory tower block or houses in a street—deals in combinations. Cities are more than just the arrangements of elements, but I would like to indulge this simplification for the purposes of this chapter, which is to establish further consonance between cryptography and the city.

Throughout this book I will refer to the *hash*, which is a prominent term in computing and cryptography. According to the OED, the *hash is* "so called because it consists of small pieces of code arranged in an apparently jumbled and fragmented way." I'll make use of its formal definitions in chapter 10, but it is relevant to concepts of multiplicity. To hash is to chop up, to hack, a term applied readily to food (recooked and chopped meat), narcotic dried herbs (hashish), and through further linguistic coincidence resonates with software hacking as applied drudgery and routine work, low-paid piecework, and labour delivered on demand in the gig economy.[3] To hash is to arrange, rearrange, or jumble elements in such a way that they

are unrecognizable from the original arrangement. In architecture, art, and urbanism the concept of the hash most likely invokes concepts of *collage*, the deliberate or accidental arrangement of disparate elements to synthesize something new. According to architectural writer Jennifer Shields, "A collage as a work of art consists of the assembly of various fragments of materials, combined in such a way that the composition has a new meaning, not inherent in any of the individual fragments."[4]

Cryptography relies on such seemingly random arrangements. Anyone invested in securing property or money is familiar with the combinatorial complexity involved in opening a combination lock, getting through a security door, or releasing funds from a debit card account. The odds of gaining access by entering numbers randomly are diminishingly slim as the number of symbols in the code increases. Cities are protected in various ways by combinations.

As I'm pressing the case for the cryptographic city, I want to discuss the combinations of city elements and combinations in security codes, and to show how they each contribute to the arrangement of cities. Combinations not only are characteristics of access systems but also are endemic to the organization of the city.

In a chapter appropriately titled "Deciphering and the Exhaustion of Recombination" in her book on cultures of cryptography, Katherine Ellison states: "These material methods of transmitting intelligence illustrate the creativity of recombination and repurposing; books and bodies are manipulated so that their parts serve diverse functions; the familiar is disassembled and recombined to produce something new and only discernible to the senses trained to perceive it."[5] The novelty engendered by combinations and recombinations provides opportunities for hiding and disguising things, in books and in cabinets with secret compartments.[6]

If disassembling and recombining cabinets and texts serves to both hide things and to create something new, then so does the city. Add to this affordance the security aspects of recombination. Multiplying and compounding compartments and rooms provides a means of increasing the security of a place. As I'll show in chapter 11 on obfuscation and espionage, multiplication serves as a means of planting confusion, which is in turn a security measure. Confronted with an array of hundreds of hotel rooms or offices, an assailant would have to undertake some effort to find the target by searching every room.

Urban Combinatorics

Consider a basic security device, a physical combination lock. A combination lock is made up of a series of metal disks with grooves and notches in them. The disks move freely around a common axis but there is only one alignment of the disks that will permit free movement of a spindle in order to engage or release a catch. Key-operated pin-and-tumbler locks work on a similar principle of alignment. The combination of notches and grooves along the key have to correspond to the position of a row of spring-loaded pins of different lengths in the locking mechanism. When you slide your key into the lock you position it within a cylinder. The correct key in the lock allows the cylinder to rotate and engage or release the latch.

Elements rotating around an axis and locking into place are invisible in everyday lock and key operations, but it's a visual trope in sci-fi and fantasy. I'm thinking of *Indiana Jones and the Kingdom of the Crystal Skull* (dir. Steven Spielberg, 2008) and *The Mummy* (dir. Stephen Sommers, 1999) as the explorers finally put the last parts of the key together to cause a panel to rotate and reveal the secret treasure. The film *Army of Thieves* (dir. Matthias Schweighöfer, 2021) fixates on cylindrical lock-and-pin movements as the virtual camera flies through the mechanisms of a series of safes that are themed on Wagner's *Ring Cycle*. I think also of architecture: the Nakagin Capsule Tower by Kisho Kurokawa and the Shizuoka Press and Broadcasting Tower by Kenzo Tange and others of the Metabolist school.[7] Nothing moves, but the living pods are locked into place around a central service axis as if they could.

The numbers visible on the spindle of a combination lock constitute a key, as do the invisible pin lengths on a key-operated pin-and-tumbler lock. As evidence of some people's fascination with locks consider those who have turned picking locks into a hobby. TOOOL stands for The Open Organisation Of Lockpickers. They hold an annual event called LockCon. The organization distances itself from criminality, actual breaking and entering. It provides instructions and runs competitions as a kind of "door hardware sport," according to their website. But the main source of fascination resides with the idea of the lock as a puzzle to be solved: "Lockpickers see locks as puzzles, and solving such a puzzle provides an enormous thrill ;-) This thrill motivates people to carry on with it, and try an even more difficult lock. It is addictive, but pacifying all the same."[8] They also claim

to expose vulnerabilities in manufactured locking systems. They thereby claim to provide a public service, also helping people who have legitimately lost their key to the front door or safe. The group admits, and seems to enjoy, that it is under suspicion, and they claim that agents of the law attend their events under cover. That the organization presents as a puzzle to others heightens the thrill.

Combinations are of interest as puzzles to architects and planners, and not just as they labor over key schedules.[9] Think of the arrangement of rooms in a floor plan, perhaps a hospital floor plan, with many functions, relationships, and constraints. Drawing an analogy with locks we might think that one arrangement provides the answer, the solution, the key to the planning problem. Floor plans are also a bit like jigsaw puzzles. But in a jigsaw, there's only one combination of spatial elements (jigsaw pieces) that reveals the (hidden) picture, the solution to the puzzle. In the case of floor plans there's not a single combination that affords a single best arrangement, a solution. Nor are all rules and criteria for the method of combination clear at the outset. We tend to think of a combination that provides an optimal condition, the best arrangement all things considered.[10] That's an operation in combinatorial complexity, though substantially less precise and well defined than arranging jigsaw pieces or aligning spring-loaded pins in a lock to allow a cylinder to rotate. Planners, designers, politicians, developers, citizens, and the forces of nature configure, organize and disorganize cities as combinations. By this formalist analogy, combinatorial complexity runs deep in the structure of the city.

To combine and enumerate are mainstays of puzzles, and of much that people think of as rationality. In chapter 3 I alluded to clues and evidence in the environment as triggers by which we recognize affordances, as part of the "code" of a place. In a forensic context those clues have to be pieced together, combined, recombined, and filtered. The writer Arthur Conan Doyle had Sherlock Holmes assert, "When you have eliminated the impossible, whatever remains, however improbable, must be the truth"[11] One of the ways to eliminate the impossible is to first enumerate everything, that is, all possible event sequences and motivations that can be enumerated—probable or not. The doyen of rationalism René Descartes said something similar. His last rule for sound reasoning "was to make such complete enumerations and such general reviews that I should be sure to have omitted nothing."[12]

It is as if the solution to a philosophical puzzle is to lay out all the possibilities and in all combinations in order to alight on the most clear-sighted. Cartesian rationality was one of the pillars of systems theory and those scholars of the Design Methods Movement who would seek such orderly, mathematical, and logical procedures for designing buildings and laying out cities.[13]

Lionel March was a pioneer in mathematical methods applied to architecture and design, among other notable contributions. His 1971 book with Philip Steadman, *The Geometry of Environment*, and subsequent books and articles makes clear the value of combination and enumeration, laying out all possibilities and permutations.[14] *The Geometry of Environment* incorporated the New Math of the 1960s and *set theory* into thinking about architecture and space. Their study was directed mainly at floor plan layouts: enumerating the possible ways that rooms can be arranged in a building taking account of adjacencies and connecting doorways. As a more abstract challenge, this could be all the ways that a rectangle can be divided into a series of tightly packed smaller rectangles. They called the process "rectangular dissection."[15] Once all possibilities are enumerated, it is then possible to count, classify, order, and filter such arrangements, and derive their properties. Such enumeration is also something you can program computers to do.

Then there's the challenge of permuting very large numbers of elements such as rectangular rooms. According to Bloch and Krishnamurti working on a similar project, there are over 280,000 ways that just ten rooms can be arranged bounded within a rectangular perimeter and ignoring room dimensions.[16] For greater numbers of rooms the number of possibilities becomes unwieldy to enumerate and process.

Under the influence of *The Geometry of Environment*, those of us with a computational bent were fascinated by the idea of enumerating all possible combinations of building elements, such as rooms in a floor plan, classifying them, filtering and selecting from all possible permutations. I had my own foray into rectangular dissections, and an attempt to deal with large numbers of rooms that meet some kinds of relational constraints as I outlined in *Logic Models of Design*[17] (figure 4.1).

By most accounts, in spite of Descartes' formulation, rational thought does not actually proceed by way of exhaustive enumeration and combination.[18] Considering the difficulties of such enumerations, and questions

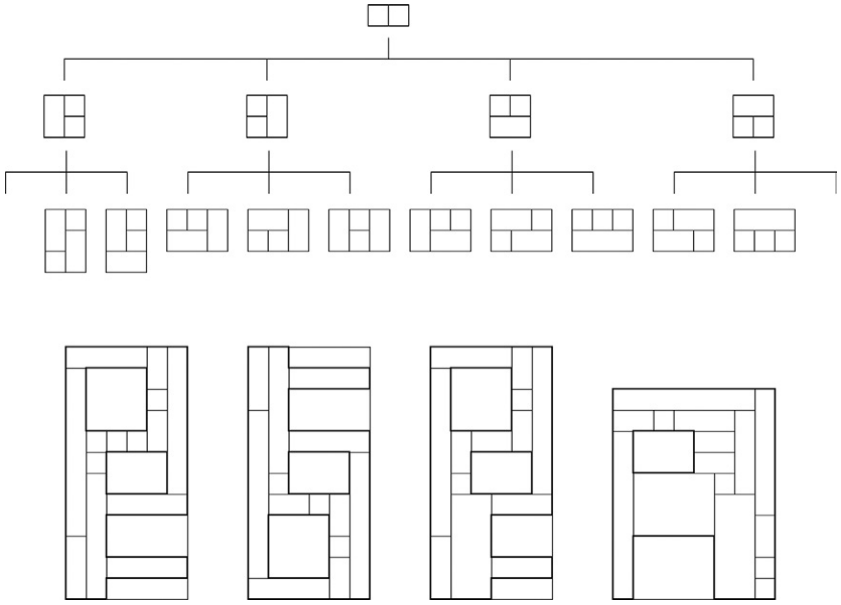


Figure 4.1
The start of a derivation tree of rectangular dissections resulting in spatial combinations of rooms and courtyards in plan. *Source:* Author.

about their practical usefulness, one may well ask what motivates such an interest in enumerating combinations of elements in architecture and urbanism. From a phenomenological and psychological point of view, I propose that apart from any practical use, such enumeration fulfills several human needs and desires relevant to my analysis of the cryptographic city.

A Phenomenology of Combinations

First, consider the need to collect and classify, which in turn demonstrates a desire to have mastery over a domain of expertise. If you can enumerate, then you can control. I mentioned the research of Walter Ong in chapter 2. In his account of the European trajectory toward organization and the pretense of rationality we see double-entry bookkeeping, but also the classification of information and knowledge, and the emergence of the encyclopedia as a teaching tool.[19] Such cultural innovations were in the company of botanical and animal classification, enumerations of architectural styles

and urban typologies, and other manifestations of encyclopedism. Laying things out in order is a way of exercising control.

Second, we are drawn by the allure of rhythm: seeing patterns, repeated patterns, and repetition in patterns.[20] Enumeration of combinations sets up a rhythm as in a production line, a poem, music, or a riddle.

Third, we're motivated by the anxiety that we'll miss something essential. As Descartes said, he thought it necessary in his philosophical reflections to provide such complete enumerations to "be sure to have omitted nothing."[21] Descartes couched his *Discourse on Method* in terms of self-referential anxiety. Fear of missing out is a basic human trait. It is the elusive combination that drives the restless generation of yet more permutations, and the search for answers and "solutions."

Fourth, we may be afraid we'll fail to find the crucial combination, the key to the safe as it were. Combinations provide a key to unlock something hidden, as in the case of a puzzle. Combinations provide a way of concealing and revealing mysteries, and of making the ordinary mysterious. The impulse to enumerate participates in the mindset of the habitual gambler: how many combinations of cards can there be before I hit on a royal flush? There's a moment in the Korean horror series *Squid Game* (dir. Hwang Dong-hyuk, 2021) where the characters have to cross a bridge made of adjacent pairs of glass panels. Only one of each pair of panels is safe to stand on. At one moment in the perilous crossing one of the characters positioned partway along the bridge realizes the extremely slim odds he has of getting to the end. He has fifteen pairs of panels in front of him. Terrified, he realizes his chance of survival is "two to the power of fifteen. . . . That's a 1-in-32,768 chance!"[22] Sometimes finding the right combination against the odds is a matter of survival and ignorance of the odds provides false comfort in the face of the inevitable.

Combinations and Riddles

Riddles operate via combination and permutations. The Sphinx was a mythic trickster, a riddler, that guarded the gate to the city of Thebes and required travelers to answer a trick question before gaining access to the city. Here, the riddle serves as a passcode. Riddles typically present as permutations, a combination of elements, albeit for small numbers, usually around 2, 3, or 4, or at least a subset of possible combinations. The Riddle of the

Sphinx asked, "What is the creature that walks on four legs in the morning, two legs at noon and three in the evening?" The riddle draws on permutations of morning, noon, and evening and the number sequence 2, 3, and 4. By most accounts, the key to resolving the riddle is to appreciate that morning, noon, and evening could apply to the early, middle, and final stages of life, and that "legs" could apply to arms and walking sticks as well. So, the resolution to the riddle of the Sphinx presented to the traveler is "a man."[23]

Urban combinatorics, or assembly, is not only a matter of deriving the best solution as if solving a puzzle. Permutations increase the chances of encountering an incongruity. After all, it was the tactic of the Surrealists to rearrange and juxtapose familiar elements in unfamiliar (incongruous) ways, as collage. They felt no embarrassment in combining sand dunes, obelisks, and crucifixes with elephants on stilts.[24] The permuted riddle format of the Sphinx also fulfills the criterion of incongruity. The permutations selected for the Sphinx riddle work as an exercise in incongruity, if not absurdity.

A senior citizen with a walking stick is less engaging as a resolution to a riddle in the current age. Poking umbrellas up chimneys has greater potential: What goes up a chimney down but cannot go down a chimney up? That's also a riddle that begins with permutations—of "up" and "down." To the child it's the combinatorial, repetitive, and rhythmical aspect of the riddle space that provides the initial appeal—even before the child appreciates the mechanics of the circumstances, and the ambiguity and its resolution that provide the sense of the absurd, and a joke.

I'm here considering riddles because they involve permutations and combinations. It is satisfying to think that with all its mathematical complexity, contemporary cryptography begins with the riddle, or at least a myth (of the Sphinx) involving a riddle as a rudimentary combinatorial challenge. Riddles are a kind of puzzle or key. After all, the Sphinx required an answer to the riddle before the traveler could enter the city. To enter the city, you had to answer the riddle correctly—or die trying. The challenge was not to establish a correct combination, but to provide a key, the answer, that ensured that the combination made sense, and resolved or enhanced the incongruity.

By one theory, the transition from the incongruity in the statement of the riddle to a resolution constitutes an aha moment. The transition from confusion to clarity provides a moment of enlightenment, satisfaction, pleasure, and even delight.[25] The riddle also presents something extraordinary,

impossible, or monstrous, like the Sphinx itself—a lion with the face of a human being—and transitions to something reassuringly ordinary.

To reiterate the role of combinatorial intricacy in the urban context, buildings and cities involve combinations of elements, spaces, rooms, furniture, and functions. In this respect they form the basis of a riddle, or at least a puzzle. A floor plan follows the format of a kind of puzzle, as a designer creates it, and as visitors move through it. The experience of the city also presents as a riddle, at least for the first-time visitor. Movement through a city can have such a character—moments of confusion followed by moments of clarity. Confusing, disorienting or jumbled spaces transition to open, clear, ordered places. Permutations of elements in the visual field that present contradictions transition to an overview that shows that the whole place makes sense after all. Think of moving through the tangle of streets in an old medieval city, and the need felt by the fit and able to climb to the top of a tower to see how the city looks from above, to make sense of the jumble of relationships experienced at ground level and discover that the cathedral is around the corner from the town hall, which is adjacent to the cafe you just visited. There's pleasure in that, the contrast and the transition—like solving a riddle.

Hacking the Combination

I have mentioned the Bletchley Park codebreaking project a few times. It provides a potent illustration of the combinatorial challenge that has cryptography at its focus. The UK's World War II codebreaking headquarters at Bletchley Park opened to the public in 1994. Those of us with an interest in computing went there to pay homage and to see the ranks of humble low-rise buildings and examine firsthand some of the codebreaking devices, to learn and to imbibe the enthusiasm for cryptography and cryptanalysis of the volunteers who populated this living museum.

The Bletchley Park museum teaches us that during World War II German operatives at command stations would be handed messages to be encrypted before relaying them via Morse code to U-boat commanders. The operative would enter each character of the plain text message into a tabletop machine—the commercially produced Enigma machine—that looks something like a typewriter. With each key stroke, a different letter from the one pressed would illuminate on a panel at the top of the machine. An

operative would have to write down the new characters as they appeared. The message so encrypted would then be sent in Morse code via conventional telegraph to the recipient, who would then decrypt the message by means of a similar machine, and a similar process. It didn't matter to the sender and recipient that the telegraph service could be tapped, as the interceptor would only pick up an apparently random sequence of characters.

The Enigma machine didn't map every character in a unique and predictable way, as if every "T" got encrypted as a "P" as in a substitution cipher. That would be trivial to decrypt. Each character was translated through several scrambling operations involving a series of disks that rotated with each press of the keyboard. The machine operation was a version of Alberti's cipher disk mechanism, though the disks would move relative to each other with each letter. The message recipient could decrypt the message as long as they had the same Enigma machine, with the same disks in the same positions, the same starting conditions, and the same circuit. The sender and receiver also had the same code book, which listed the required parameters for the machine on any particular day. Any interceptor with a similar Enigma machine and the code for the day could decrypt any messages they picked up.

The codebreaker challenge for the Allies as cryptanalysts was to develop a system for deriving the code for the day. This required cunning, experimentation, and electromechanical devices that could iterate through very large combinations of parameter configurations. The first such machine was known as "the Bombe," a proto computer. It was crucial that the Germans did not know how their messages were intercepted. A few changes in the encryption method would have meant the codebreakers would have to revise their methods to uncover that. As I outlined in chapter 3, as well as the contest of a devastating war, cryptography itself was a site of contest between coders and codebreakers. It was also a contest against combinatorial complexity. Bletchley Park is a reminder of how the securing of secret information relies on the sheer quantity of possible combinations of numbers, symbols, and sequences.

Counting Characters

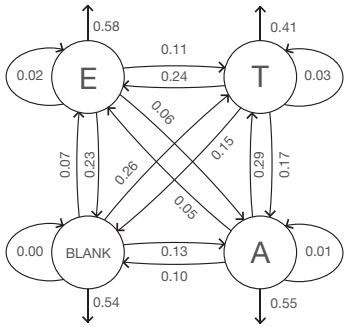
Combinatorial complexity is one of the means of confounding codebreakers. But consider how codebreakers have exploited the combinatorial aspects

of language, understood through letter frequencies. As I have shown, a substitution cipher is one of the simplest methods for encrypting a message. A unique symbol stands in place of each letter in the hidden plain text message. The symbol set can consist of any arbitrary set of characters, as long as each symbol maps uniquely to the letters of whatever alphabet you are using for the plain text message. The usual encryption method is to deploy a different letter from the same alphabet, so that the encrypted message contains the same character set as the hidden message (e.g., the twenty-six letters of the English alphabet A to Z plus a space). This method is often referred to as the Caesar cipher. It is also the method deployed in the Masonic (pigpen) cipher and Wittgenstein's cipher.

As known to any Scrabble player, letters in a block of text occur at different frequencies. For example, E is more common than Q. Letter frequency provides a clue to decrypting a coded message. If the frequency of the letter E is 12.1 percent, then the probability that the letter E will show up in any position in a coded string is 0.121. On the *Practical Cryptography* website, James Lyons provides a helpful blog post with the frequencies of letters and in various combinations.[26] As text messages are sequences of characters, it would also be useful to know the probability that any letter will be followed by any other letter. How often is an E followed by another E, or an S or D, and any other letter? According to Lyon's frequency data, in any block of text you can expect the letters EE to occur in 3.54 percent of all adjacent pairs of letters, ES occurs 1.32 percent of the time and ED 1.08 percent of the time. I calculated these percentages from Lyons's letter frequency data.

A cryptanalyst might also want to know the frequency with which, given an E, the next letter will also be an E, an S or a D, and so on. With that statistical data we can produce probabilities that populate a transition matrix, that is, a table showing all the letters of the alphabet plus the space character, and the probabilities that any letter will be followed by any other, including itself. That information can also be understood as a transition network with twenty-six nodes and a tangle of connecting arrows connecting each node—and with probabilities attached. I show a more manageable subset of the challenge in figure 4.2.

This information about the probability that one particular letter will be followed by another particular letter provides the ingredients for a Hidden Markov Model (HMM) formulation of the problem of automatically deciphering a substitution cipher. In HMM terms, the hidden part is the path



	E	T	A	O	I	N	S	BLANK
E	0.02	0.11	0.06	0.03	0.03	0.21	0.30	0.23
T	0.24	0.03	0.17	0.14	0.13	0.00	0.12	0.15
A	0.05	0.29	0.01	0.01	0.05	0.29	0.19	0.10
O	0.03	0.15	0.06	0.09	0.04	0.41	0.14	0.06
I	0.12	0.12	0.09	0.10	0.00	0.35	0.15	0.07
N	0.20	0.13	0.14	0.11	0 07	0.07	0.15	0.13
S	0.16	0.17	0.07	0.05	0 07	0.02	0.04	0.42
BLANK	0.07	0.26	0.13	0.06	0 06	0.14	0.27	0.00

Figure 4.2
Transition network and table. The network on the left shows the three most frequently occurring letters (and a blank space) in the English language, and the probabilities that one letter will follow another in a word. The table shows the same information for the seven most common letters. The probabilities here are derived from anagrams of ETAOINS generated at unscramblex.com. The matrix and network would be much larger for all the letters of the alphabet. Such sequence representations are useful in codebreaking, DNA sequencing, weather prediction, machine learning, and other applications of Hidden Markov Models (HMM). *Source:* Author.

through a network of twenty-six letters (plus space) that make up the order of letters in the hidden message. The observation part of the HMM formulation is the encrypted version of the message. I'll also say more about Markov models in chapter 12. Here, it is sufficient to note that information about the frequencies of letters, and the frequency of particular combinations and sequences of letters forms part of a typical codebreaking toolkit.

The variation in letter frequency was important initially in movable type printing. You needed more Es than Qs, so a printer's "type case" would need a bigger compartment to hold the letters. Figure 4.3 shows an image of a type case that spatializes letter frequency as something that looks almost like a city block or item of furniture.

Calculating the letter frequency in a block of text provides a way of making a good guess at the language it's written in—automatically. An interesting website at letterfrequency.org provides the frequency order of letters in a range of languages.[27] For example, the frequency order in English starts "ETAOIN . . ." In German it starts "ENISRAT . . ." In French it's "ESAITN . . ."

In the 1950s, the pioneering information scientist Herbert Ohlman ran calculations on sets of texts to determine the relative frequencies of letters.[28] He calculated the frequencies in different parts of words: the first,

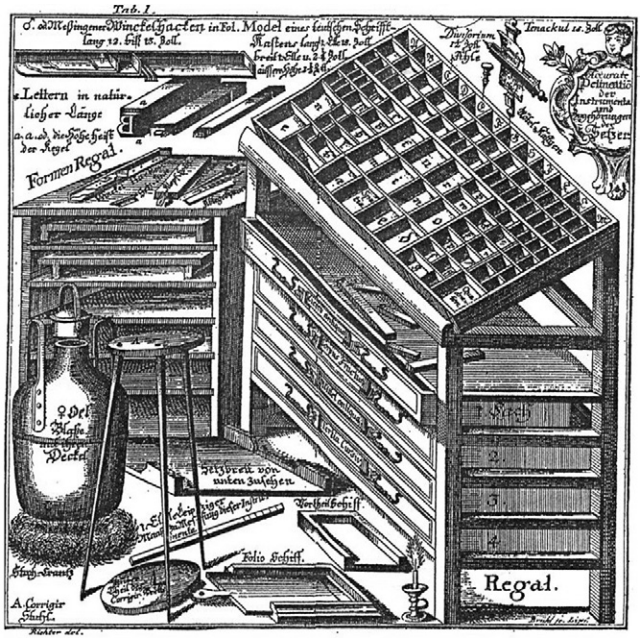


Figure 4.3
An eighteenth-century "type case" that spatializes letter frequency. The drawing is captioned: "By Christian Friedrich Gessner—Illustration taken from a scan of: Christian Friedrich Gessner, 'Die so nöthig als nützliche Buchdruckerkunst und Schriftgiesserey: mit ihren Schriften, Formaten und allen dazu gehörigen Instrumenten abgebildet auch klärlich beschrieben, und nebst einer kurzgefassten Erzählung vom Ursprung und Fortgang der Buchdruckerkunst'" (1740), 226f, and is in the public domain via https://commons.wikimedia.org/w/index.php?curid=13538088.

second, third, fourth, and fifth positions. If we need any further support for the importance of cryptography, Ohlman also asserted: "Coding, or the transforming of information from one guise to another, is one of man's commonest activities. Every picture may be said to be a coding of some real scene and every written word a coding of some utterance—the brain itself is said to work with coded impulses."[29]

Encryption Keys

Cryptography reduces combinatorial complexity for the sender and receiver by the use of keys. For my purpose here it is sufficient to note that

the operations of public and private encryption keys continue this story about combinatorial complexity. In the rest of this chapter I'll explore the basics of their operation for any reader who shares my enthusiasm for the instruments of codes and permutations. So what follows in this chapter will involve some technical detail.

It is easy to grasp the idea that you need a key to gain access to a safety deposit box or a room to access something that someone wants to keep secret. The answer to the Riddle of the Sphinx is a key, which in turn gives access to the bridge and the city beyond. Cryptographic keys are a means of turning a seemingly arbitrary combination of characters into something comprehensible in plain text.

Consider a simple substitution cipher. The message is encrypted simply by replacing each letter in the text with the letter that appears a certain number of characters further on in the alphabet. For this purpose, the alphabet is placed around a circle so that it returns on itself. If the displacement is 4 then the characters ABC appear encrypted as EFG. Ignoring spaces, the message such as "WRITE ME A CITY" would appear as "AVMXIQIEGMXC." The key to decrypt this particular message is simply the numeral "4." The recipient just has to know that the key is the number 4 to apply the simple algorithm of counting back that number of letters. That is not very secure, however, and is easy for codebreakers to intercept without the key. They just need to keep adding or subtracting integers to work their way through positions in the alphabet until they stumble across a sequence of letters that looks like a coherent string of plain text. As well as letter frequency, codebreakers can exploit information about letters less likely to appear in pairs, such as A, H, I, J, K, Q, U, W, and Y.

Instead of a single number for the displacement key the encryptor could specify a series of numbers repeated across the message. A ten-digit key would increase substantially the degree of difficult for a codebreaker. So, a key 1437823605 means count up the alphabet 1 for the first character, 4 for the second, 3 for the third, and so on. That's like a rotating combination key on a padlock. The key then repeats for the rest of the coded message to turn my original plain text message into "XVLAMOAGCNUC." That would be impossible to decipher in a reasonable time using paper and pencil, though not for a computer iterating through every possible combination of numbers for a ten-digit key.[30]

Alphanumeric data is stored and transmitted in binary, as series of 1s and 0s. So, the counting process for the substitution cipher is replaced by flipping binary bits according to the sequence in a binary key. In this case the key is a series of 1s and 0s. Most digital encryption now uses 256-bit encryption keys. Cybersecurity expert Jon Watson provides a helpful explanation of the process that involves multiple iterations to effectively scramble the 1s and 0s, though in a way that allows the receiver to use the original sequence to restore the message with the same key.[31]

What I have described here is known as symmetric key encryption. The sender and the receiver of the message (i.e., the sender's and receiver's computers) use the same key. The AES (advanced encryption standard) is developed around this method. One of the main vulnerabilities of this approach is that the encryption key must be shared between the communicating computers before they can generate and transmit their encrypted messages to one another. The encryption key will need to be communicated via an insecure, or less secure, connection. If someone intercepts that transmission, then they will have the key and can decrypt the secret messages. It also means that the sender and receiver are both custodians of the key, and each will have a different stake in its security. So it is vulnerable. That's like giving a copy of your house key to someone to collect your mail while you are away. As the owner of the house I am likely to be more vigilant about protecting the key than the mail collecting friend would be.

Public Key Encryption

Public key encryption, also known as asymmetric key encryption, offers a solution to the problem of transmitting cryptographic keys across unsecured networks, the so-called "key exchange problem." In this method, the key to encrypt a message is different from the key used for decrypting it. It doesn't matter if other people intercept or even use the same encryption key as you do because that key cannot be used to reverse the encryption process.

The complicated chaining and nesting of access privileges in securing the exchange of data has spatial correlates. Various metaphors come to mind for public key encryption. It is as if you and your friends have identical keys that open the letter slot in your front doors. That is the public key.

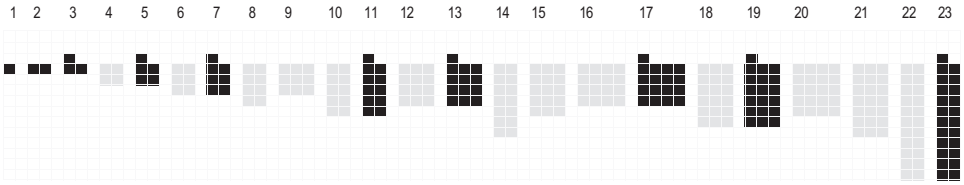


Figure 4.4
Spatial representation of the first ten prime numbers (in black). Public key encryption uses very large primes. *Source:* Author.

Any of these key holders can open the letter slot of any of the houses and drop a parcel into the house, but only the owner of the house has a key that gives one person access to the house, the owner. That is the private key. Once inside they can access the parcel.

How is this kind of security implemented in the case of digital data? Large numbers secure data: not just any large numbers, but primes. Digital public key encryption systems commonly deploy algorithms that exploit the properties of prime numbers to encrypt a message. A prime number is a positive integer that is not the product of two other integers (except 1 or itself). If you try and draw a rectangle on a regular grid that only takes up a prime number of grid units, there will always be at least a grid cell left over. Prime numbers are always odd (apart from the number 2). You can always turn a prime into a non-prime (i.e., a composite) by subtracting 1 from it (except for the first three primes in the series). As I'm keen to keep this account spatially relevant, I show the first ten primes as grids of squares in black in figure 4.4.

It is easy to multiply two numbers, even if very large, but more difficult to factor a number, meaning to find two numbers that when multiplied result in that number. It is especially difficult if the two numbers multiplied are primes. They will be the unique factors of their product. There is only one solution to the factor challenge for a number so produced. Factoring is a trivial calculation for small prime products, for example, the prime factors of 35 are 7 and 5 and only those two numbers. But factoring is computationally taxing for prime products over one hundred digits long.

Public key encryption requires two numbers: a public key number and a private key number. A helpful blog post by Nick Sullivan explains that "you can take a number, multiply it by itself a number of times to get a

random-looking number, then multiply that number by itself a secret number of times to get back to the original number."[32] By "large numbers" cryptographers mean numbers in the order of four hundred digits. A helpful tutorial paper by Kathryn Mann amplifies further the scale of the combinatorial challenge: "The lifetime of the universe is approximately 10^{18} seconds—an eighteen-digit number. Assuming a computer could test one million factorizations per second, in the lifetime of the universe it could check 10^{24} possibilities. But for a four-hundred-digit product, there are 10^{200} possibilities. This means the computer would have to run for 10^{176} times the life of the universe to factor the large number."[33]

Here is some detail about the process. Person B (Bob) wants to send person A (Alice) a secret message and therefore asks A for A's public encryption key. Person A transmits A's public encryption key to B to facilitate this. Person B uses that public key information to encode a message according to the algorithm described as follows. Person A has the private key and can decode the message. Three items are transferred in sequence.[34]

1. B's initial low-security request for A's public key.
2. The public key transferred from A to B, which is low risk. It doesn't matter if hacker C (Eve) intercepts that transfer and finds out what the public key is. All that would enable C to do at best is to encrypt a message, not to decrypt a message.
3. The encrypted message from B to A, which is secure. A can read this with the private encryption key. The message could only be read by C if C had the private key. The private key is never transmitted and stays with A.

The algorithm behind this method of public key encryption is called RSA encryption after the three inventors, Ron Rivest, Adi Shamir, and Leonard Adleman.[35] These operations are of course invisible to the computer user and are the kinds of operations carried out by browser and server software in requesting and transmitting information securely across the Internet. The keys are also invisible to the users.

If it is not obvious by now, the encryption key is different from the short passcode that the user needs to access their computer, online banking, or account on a website. Passcodes are themselves encrypted before they get passed though the network to password servers that contain password lookup tables, which are in turn in a kind of code (a hash).

Combinations and Trapdoors

Public key encryption is like a turnstile or trapdoor, a one-way portal. You can go through it easily in one direction, but it is difficult to come out again in the reverse direction. A horizontal trapdoor relies on gravity for the one-way function. It is easy to fall through it into the cellar below, but harder to jump or climb your way out. That is similar to the way hunters use pits to trap prey, and some insects lure prey into a one-way system from which there's no escape. Trapdoors associate with secrets and hiddenness. A stage magician will install a secret trapdoor under a magic box. The assistant falls through the secret door before the magician opens the lid to reveal the box is now empty.

Cryptographers use the trapdoor metaphor to describe their methods. It is easy to encrypt a message, but has to be substantially more difficult to recover it without a special key, or escape route, as in the case of factoring a number into primes. It is easy to get the toothpaste out of the tube, but more difficult to get it back in. The main lessons from this mathematical exposition are that digital encryption takes advantage of combinations of number sequences, the irreversibility of some cunning mathematical operations, and the impossibly long odds of finding the right combination without clues, keys, and knowing the procedures and information about some essential parameters.

It's worth concluding this discussion with a further means of securing the process and some elegant mathematics. The multiplication of prime numbers can be made even more difficult to unmultiply if you redefine multiplication. One method is to define multiplication in terms of geometrical relationships between points on a curved line. Elliptic curves belong to a family of curves that make up the alluring surfaces of much contemporary organically inspired architecture. They are also the basis of encryption methods that secure digital communications. Mark Hughes provides a very helpful explanation of the Elliptic Curve Diffie–Hellman key exchange[36] that operates with primes and modular arithmetic. I provide an explanation that brings out some of the elegance of the curve geometries in some of my own online explorations.[37] I provide one of the diagrams in figure 4.5. If your computer and my computer are to communicate in secret then they need to agree to use the same elliptic curve, with the same parameters.

A great deal of modern cryptography is based upon the Diffie–Hellman key exchange, which requires that two parties combine their messages with

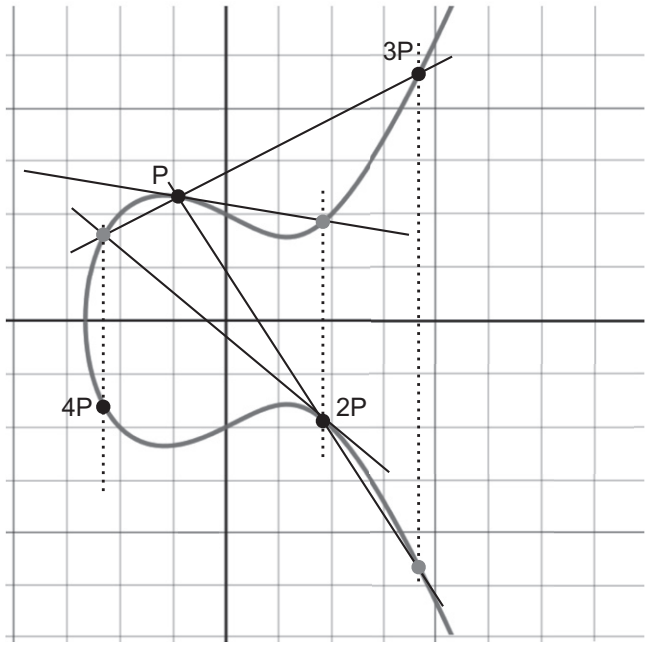


Figure 4.5
Elliptic curve with the general formula $y^2 = x^3 — ax + b$. It is possible to draw a straight line through two points on this curve that will only strike one other point on the same curve. Factoring into prime numbers is made even more difficult when multiplication is defined in terms of intersecting vectors on this curve. *Source:* Author.

a shared secret that is difficult for a bad actor to deduce. The Elliptic Curve Diffie–Hellman key exchange method allows microprocessors to securely determine a shared secret key while making it extremely difficult for an eavesdropper (Eve) to discover that same shared key. The method uses modular arithmetic commonly described as numbers that "wrap around" as on a clock face. A clock face has a "modulus" of 12. The prime number multipliers our computers choose for our private keys will also be many digits long as will the modulus and the coordinates of the initial point on the curve for the sequence of calculations, further securing the method.

Misplacing Words

Of necessity this has been a brief overview of important encryption methods. My main aim was to focus on combinations and how they can secure

data flows. They entail operations in common with combinatorial puzzles. This chapter also introduced a series of metaphors: puzzles, riddles, locks, keys, cabinets, rooms, trapdoors, turnstiles, toothpaste. A metaphor serves as a means of explaining abstract and complicated processes. Metaphors also run deep and permeate the geometry and mathematics of encryption—to the extent that explanations and functional operations become the same.[38] The urban lifeworld provides metaphors for understanding cryptography and vice versa. It is tempting to say that the "cryptographic city" is just a metaphor, but considering the depth of metaphor in understanding and making the world metaphor simply reinforces the connection.

Metaphor usage is also an exercise in combination and recombination. In a class on metaphor and UX design I allocate random nouns to groups of students and invite them to combine pairs of words to create a concept for a game, a song, or a productivity app: cloud-brush, shower-hinge, umbrella-book. It requires little effort to imagine something interesting, no matter how ridiculous. In any case, metaphor also implies a transgression. To employ a metaphor is to engage in a kind misclassification.[39]

I'm prepared to place theft within the same metaphorical understanding. Cryptography aims to secure objects, places, and data against theft. To steal data is to recategorize what's yours as mine. Were it not for the despair and inconvenience we could see data theft as a profound exercise in the metaphorical imagination—or at least we can learn from it as such.

In *A Burglar's Guide to the City* Manaugh writes about a "hidden topological dimension tucked away inside the city."[40] Thinking of the clever bank heist that involves traversing rooftops, negotiating tunnels, and boring holes in walls, he suggests that "point A might illicitly be connected to point B"[41]; the burglar has to "make this link real" by means of "shortcuts, splices, and wormholes."[42] Criminal conjuring gives the illusion of spatial and temporal paradox: "Burglary reveals that every building, all along, has actually been a puzzle . . . a kind of intellectual game that surrounds us at all times and that any one of us can play."[43] This proposition that place is a puzzle adds further support for my assertions that the cryptographic city is a site of combinatorial practices, arranging and rearranging. Translating the theft of physical objects and its prevention to digital data further supports the proposition. Puzzles, hidden connections, and underground tunnels remind me of the workings of the labyrinth, the subject of the next chapter.

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