



## AI and the Cryptographic City

### Description

My book *Cryptographic City: Decoding the Smart Metropolis* (MITPress) came out in May 2023.



Here's a summary taken from the [MIT Press website](#).

Cryptography is not new to the city; in fact, it is essential to its functioning. For as long as cities have existed, communications have circulated, often in full sight, but with their messages hidden. In *Cryptographic City*, Richard Coyne explains how cryptography runs deep within the structure of the city. He shows the extent to which cities are built on secrets, their foundations now reinforced by digital encryption and cryptocurrency platforms. He also uses cryptography as a lens through which to inspect smart cities and what they deliver. Coyne sets his investigation into the cryptographic city against the backdrop of the technologies, claims, and challenges of the smart city.

Cryptography provides the means by which communications within and between citizens

and devices are kept secure. Coyne shows how all of the smart city innovations— from smart toasters to public transportation networks—are enabled by secure financial transactions, data flows, media streaming, and communications made possible by encryption. Without encryption, he says, communications between people and digital devices would be exposed for anyone to see, hack, and misdirect. He explains the relevant technicalities of cryptography and describes the practical difference it makes to frame cities as cryptographic. Interwoven throughout the book are autobiographical anecdotes, insights from Coyne’s teaching practice, and historical reports, making it accessible to the general reader.

AI features prominently in the book. Here are the relevant entries in the index.

- AI (artificial intelligence), 89, 53, 213.
- Machine learning, 92, 207, 212–213, 215
- Neural network, 212, 215

Considering my renewed optimism about the medium, I asked ChatGPT to cook up a “critical review.” Of course, it couldn’t review the whole book, just the abstract.

One strength of the book seems to lie in its comprehensive approach. By examining both the historical aspects of cryptography in cities and its modern-day applications in the context of smart cities, Coyne provides a broad perspective on the subject matter. The incorporation of autobiographical anecdotes and teaching insights adds a personal touch and may contribute to making the content accessible to a wider audience.

The review is longer, but it’s fake. So, I won’t extend the potential circulation of such artifice. Of more interest to me, I want to test ChatGPT’s competence with a simple cryptography challenge. It’s well-known that the current version of this platform isn’t designed for calculation (see [The invention of language](#)), but it is prepared to deliver the *effect* of having performed a calculation, as I will now illustrate.

## Pseudo-encryption

I asked ChatGPT to supply me with a random numeric encryption key with 6 digits. It came up with **532497**. That’s a good start. I then asked it to encrypt the word “**architecture**.” I describe the method on page 94 of the book. It’s the well-known *symmetric key* method of encryption. You take the original plain text phrase and count forward for each letter in the alphabet according to the number in the key that corresponds to each letter. So, count 5 characters from **a** to get **f**; count 3 characters from **r** to get **u**, etc. You repeat the numbers in the key across the whole message, and also treat the alphabet as a loop. So, **xyz** is followed by **abc**! ChatGPT gives the following result.

- Plaintext: a r c h i t e c t u r e
- Displacement: 5 3 2 4 9 7 5 3 2 4 9 7
- Ciphertext: f u e l r f a b v x u j

Therefore, the encrypted ciphertext for the word **architecture** using the provided displacement key (532497) is **fuelfabvxuj** in this simple substitution cipher.

That looks plausible, but a simple manual calculation with pen and paper shows that it's only correct for the first few characters of the word **architecture**.

On paper I created a further example using a different plain text mystery word to produce ciphertext with the same key. The ciphertext is **huatcvlucq**. I asked ChatGPT to decrypt this. It replied:

To decrypt the ciphertext **huatcvlucq** using the same displacement key (532497), we'll perform the reverse operation of the simple substitution cipher. Instead of shifting forward, we'll shift backward by the corresponding digit in the encryption key.

- Ciphertext: h u a t c v l u c q
- Displacement: 5 3 2 4 9 7 5 3 2 4 9 7
- Plaintext: c r y p t o l o g y

Therefore, the decrypted plaintext for the ciphertext **huatcvlucq** using the displacement key (532497) in the simple substitution cipher is **cryptology**.

Again, the result is presented in a plausible manner, but it's incorrect. The plain text I encrypted was actually **cryptogram**. I asked ChatGPT to check its calculation. It came up with another result.

- Ciphertext: h u a t c v l u c q
- Displacement: 5 3 2 4 9 7 5 3 2 4 9 7
- Plaintext: c y s p h r a t e s t e

Upon rechecking, the correct decrypted plaintext for the ciphertext **huatcvlucq** using the displacement key (532497) in the simple substitution cipher is **cysphrateste**.

Not only is this incorrect, but ChatGPT seemed to invent a new word. Irrespective of whether or not that was my plain text word, I asked if **cysphrateste** was an actual word in English. It confessed that **cysphrateste** is not and that the decryption was incorrect. (It didn't remind me that the efficacy of cryptography doesn't depend on the meanings of the words.) Out of interests, I asked it to think of a meaning for **cysphrateste** based on the etymology of its parts.

Certainly! Given that **cysphrateste** is a made-up word, we can create a speculative meaning for it based on the etymology of its parts.

Breaking down the word **cysphrateste**, we can consider potential roots or components:

1. **Cysph-** could be derived from **cypher** or **cipher**, which relates to codes, encryption, or secret writing.

2. -rate- might be associated with ratio or rate, indicating a measure or proportion.
3. -este could be a suffix reminiscent of verbs or actions.

Based on these speculative etymological components, we could propose a potential meaning for cysphrateste as follows:

Cysphrateste (noun): A calculated or proportioned encoding or encryption, typically associated with secret writing or coded communication.

A Google search reveals that these roots are made up. The platform had continued the cryptographic theme throughout this conversation, indicating the strength of its methods for retaining context. It also defaulted to the outcome from its neural network training. Its vast corpus of training texts presumably included phrases, sentences and contexts that included textual demonstrations of the cryptographic process I was expecting it to undertake, but without the capability to perform the necessary calculations or test its results.

I asked how conversational text-based AI (such as ChatGPT) might now or in the future be of use in conjunction with cryptography but that's for another post.

## Note

- Featured image is enigmatic pavement art by Astral Nadir (2017) on the streets of Melbourne. Photographed May 2023.
- I tried this cryptographic experiment with GPT3 before I subscribed to GPT4.

## Category

1. Artificial Intelligence

## Tags

1. architecture
2. artificial intelligence
3. cryptography

## Date Created

June 17, 2023

## Author

rcoyne99