Cryptography

"If everyone is thinking alike,then somebody isn't thinking."

For what it’s worth . . .

How does, "basically winning the Battle for the Atlantic" sound for importance?

- → The largest impact of the Enigma cracking was submarine warfare.
- → By cracking the Enigma code, the Allies could better predict Nazi submarines and react accordingly by altering the path of it's convoys and being better able to counteract their efforts.
- → Breaks in the Enigma's code either via mathematics, ingenuity, or even militarily, like U-571, contributed a very underrated role in keeping Allied convoys safe.
- → "Lives/supplies/money saved" is a really hard thing to calculate, and things like, "U-boats didn't find this convoy" often go unnoticed in the grand scheme of things, but have far-reaching consequences.

Why bother with this ?

So, why do we need cryptography? This isn't the same as asking why we need encryption. That's obvious and uninteresting: sometimes we want to communicate with others without other people knowing what we're saying. We don't want people to know my credit card number when we buy something on Amazon, for example.

I'm asking why we need cryptography, *a disciplined study of codes*?

Why can't we just roll our own intuitive, simple mechanism for encrypting information so that it can only be read by our intended recipient?
Interestingly, people have been trying *and failing* to securely encrypt information for 1000s of years. Moreover, many of those attempts were not grounded in any kind of rigorous way of thinking about codes. In other words, they were simple, intuitive methods of encrypting information; they were attempts at encryption without cryptography.

So that's why we need cryptography: our intuitive, simple methods of encryption provide no *guarantee* of security; security is hard.

What we're dealing with here . . .

- A pinch of Mathematics,
- Two teaspoons of programming, and
- A bucket full of dedication to break things

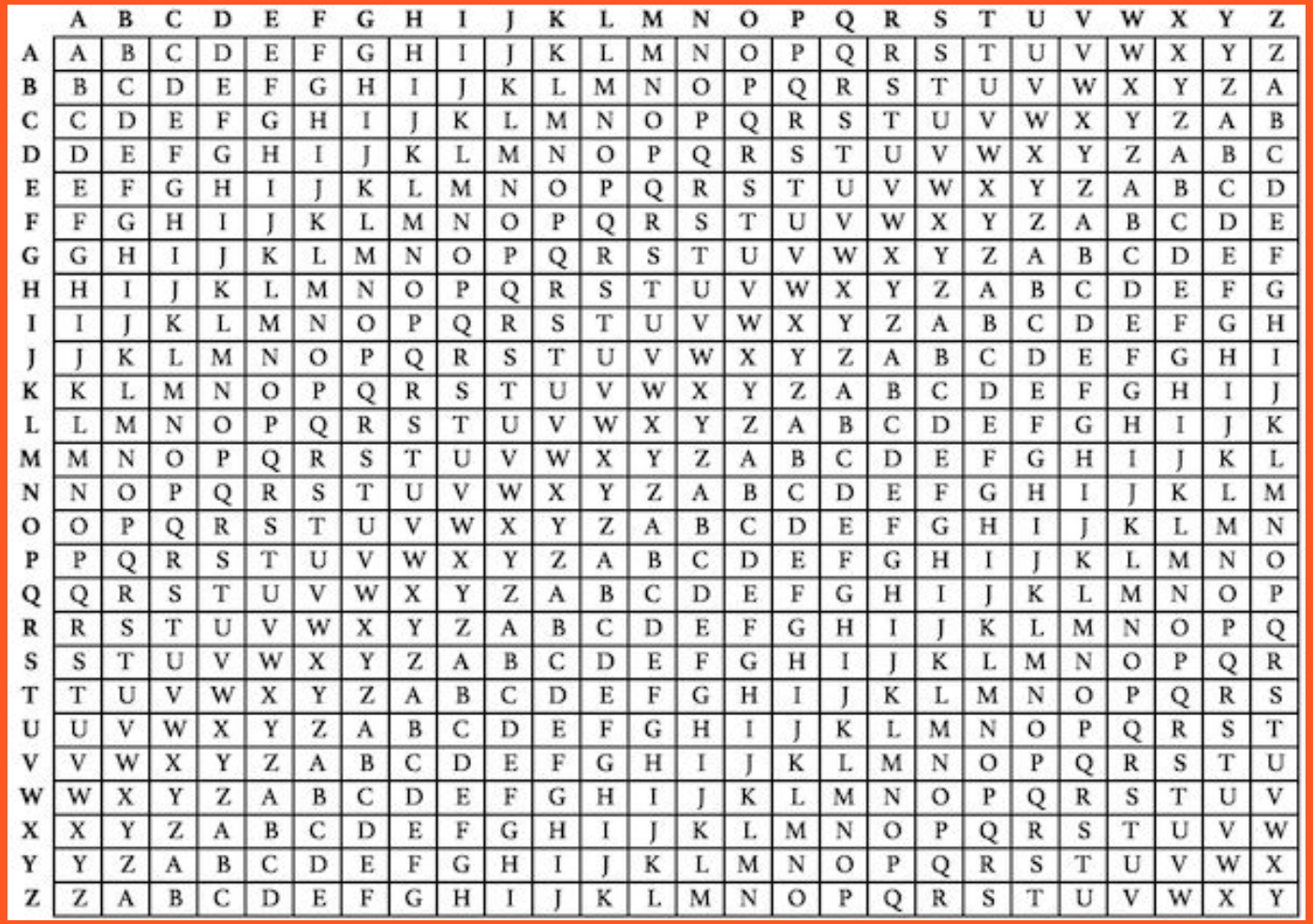
Challenge Walkthrough

Example I

Ciphertext - Nggnpx 0k01 jvyy abg or guvf fvzcyr.

Example II

Ciphertext - Jhb kl yjbx gojp ljenwg ?



What role do we play in all of this ?

Agenda

- → Introduce vital cryptography concepts
- → Attempt to solve challenges through the tools at our disposal
- → Develop proficiency in identifying real world problems and work towards a “secure” future

Where to start ?

Resources

- https://github.com/pFarb/awesome-crypto-papers
- https://github.com/sobolevn/awesome-cryptography
- https://picoctf.com/learning_guides/Book-2-Cryptography.pdf
- Cryptography I and II by Stanford on Coursera
- Crypto 101 PDF
- Hacking Secret Ciphers with Python - Al Sweigart