In this project, I will build a Wizard exe that;

* Allows data files to be encrypted and decrypted appropriately
* Includes Quantum Resistant algorithms, such as Vector, or Symmetric ones
* Explains, educationally;
  + Explains each encryption type’s methodology ( how it works )
  + It’s mathematical backing ( it’s *algorithm* algorithm, and how each part functions logistically ( picking it apart ) )
  + Why it’s included ( Historical backing & expected future implementation ( such as, why QR algorithms are important, to begin with )

In this project, I’ll be learning to;

* Create a wizard exe
* How to create an encryptor, decryptor program
* Quantum-Resistant cryptography, their algorithms, and in general, a higher level of cryptography, a field I’m passing about, to begin with
* Successfully explain important concepts in an intuitive, and creative manner (educationally)

Why this matters;

* Quantum computing is a growing field, and just like AI, it’s probably going to creep up on us, industry/sector wise, so getting ahead on Quantum-Resistant encryption algorithms is probably a good idea; and as the exe is mostly small-level in complexity ( three algorithms planned; a basic, ‘normal’ encryption method, a Quantum-Resistant one, and an unknown, relatively new one; if time IS available, more later ), it’ll serve more-as an educational tool + example tool.
* I know next to nothing about cryptography ( or, to be more precise, I know enough to know how little I know, no? ); and in fact, sort of hate it, BUT, since it’s an important field in our industry, and since I at least foresee the importance of things like this, I know diving in now will not only A; help me out in the on run; B; be a valuable skill to learn; this is a project about learning, so might as well go for keeps, no?
* On a more serious note; I know enough to know I know nothing, but even then, I know people, Globally, are going with a “take now, decrypt later” approach to large, large swaths of public, and private data. This is because, with the growing advent of Quantum Computing, previous encryption methods are bound to be cracked! Remember, encryption is basically a series of complex formulas and functions we push our data through, to encode it; a lot of them relying on large prime numbers, and the such. The issue is then, with the ridiculously high-computing power Quantum-Computers represent, those algorithms and functions we rely on are looking more like to be broken by basic brute-force methods, if anything. That’s why *resistant* ( for in this field, *nothing* is immune ) algorithms, such as Vector-Based-Encryption, symmetric-algorithms, and others, are so important; and why spreading the basic ‘what’s there to know’ is, too;

And afterall, knowing is half the battle ( lmao )

But no, seriously, this could be a serious, actual threat to people’s lives. Medical data, corporate data, governmental data; hell, every computer, phone, application, message? They’re all encrypted using algorithms with quantum computing NOT in mind. And, Quantum chips are already here? There’s already a privacy collapse going on digitally; and I’d like to endorse some awareness, and thusly, some preparation, before we hit total privacy collapse?

Although to be more honest, I hope I can look back in ten, twenty years, and say I’m dead wrong; I’ll take Y2K-2 any day, over an advent of a/the digital Chicxulub Impactor.