**PHYS379 Group 3 – Quantum Computing B**  
  
For our group project, we will be implementing two different quantum algorithms using both numerical simulations and (hopefully) actual quantum hardware via IBM’s Quantum Experience.

The first will be Grover’s Algorithm (this will be done by Willow and Ana). We will be using a variation called *Grover Adaptive Search* to find the most habitable planet in a pre-existing dataset of exoplanets. Each planet with a known mass, radius and temperature will be assigned an Earth Similarity Index (ESI). We will then use successive Grover searches to find planets that are increasingly habitable compared to a random initial planet. We will then test how accurate it is for different iteration lengths and different sized datasets (and hence different numbers of qubits). We will also compare it to a classical linear search. Since simulating a quantum computer is computationally intensive, we expect the linear search will run faster in real-time even though Grover’s Algorithm is formally quicker.

The second will be Shor’s algorithm (done by Sid and Sam). We will be proving that it is possible to break RSA encryption using Shor’s algorithm. The RSA encryption method uses the product of two large prime numbers to encode a given message and then sends the necessary decryption information via the private key. Shor’s algorithm can bypass the need for the private key by using the inverse Quantum Fourier Transform to very quickly obtain the prime factors for any given number. The aim of this project is to simulate this entire process using python using a small number of qubits (up to 10) to try and break 48-bit RSA, thus proving the possibility of breaking RSA encryption on an industrial scale, given enough qubits.

A picture containing bar chart

Description automatically generated