**How the world can be protected against the quantum computers of the future:**

The current encryption systems for information use the RSA encryption algorithm to encode data. This algorithm uses asymmetric encryption, where either the private or public key can encrypt the data and the other key can decrypt it. It involves 2 large primes being multiplied together to create an integer, n, which is then used to create both the private and public key. In order to break the key, any unauthorised user would have to deduce the 2 primes used to calculate n, and due to their large size, this is said to take classical computers approximately 19.8 quadrillion years using brute force. This is the current standard for encryption worldwide, and has protected data for over 40 years, but it is not prepared to protect against the quantum computers of the future.

Where a classical computer takes millions of aeons to decrypt the RSA encryption algorithm, it would take a quantum computer approximately 104 days to brute force the algorithm, an insignificantly small amount of time in comparison to the reward that could be achieved from cracking it. Using Shor’s algorithm, a quantum computer would be able to crack the RSA algorithm incredibly quickly, due to its ability to execute multiple calculations at once, allowing it to find the correct exponent to raise any number to such that it is equal to 1 above a multiple of n. This is the part that is the lengthiest for classical computers, as these numbers are so big, and due to being able to decrease the time taken for this step, quantum computers are thus able to crack the algorithm rapidly.

Though this many not seem to be such a large threat currently, as quantum computers are not powerful enough to do this, requiring 4000 qubits whilst the largest only contains 1121 qubits, hackers have become hopeful, and are now using the SNDL strategy - Save Now, Decrypt Later. This allows for them to save and download data now, that is still using RSA encryption, and then once quantum computers advance enough, decrypting the data. This is particularly dangerous as the data they are saving must be useful in 10 or more years for this to be worthwhile, and so hackers are downloading secret intelligence documents and important research documents, as they will still be valuable in the future.

Although quantum computers are often said to work differently to classical computers, not being necessarily better than them, this has been proved false. Quantum supremacy was achieved by Google in late 2019, conducting an experiment on a 70-qubit system that would take a supercomputer 47 years to conduct. While this is exciting, this is also alarming, as the above statement regarding the little time taken for a quantum computer to crack RSA was just a theory, supposed to be used in an ideal world with perfect fault-tolerant computers - quantum supremacy being achieved on imperfect systems proves that the theory could probably become a very real future.

Due to this theory, NIST - the National Institute of Standards and Technology in the USA, created a new competition, similar to their competition for new hash functions, this time focused on Post-Quantum, or Quantum-Safe, cryptography. Post-Quantum cryptography is often mistaken for Quantum cryptography, and while both very powerful and secure, they are completely different. Quantum cryptography is cryptography produced by a quantum computer to be run on a quantum computer, and is incredibly powerful and secure, as the qubits can only be measured in 1 state, whilst the key may be any of the other states the qubit is currently superposed in. Post-Quantum cryptography, however, is cryptography produced by classical computers to be run on classical computers, but to protect against the incredibly rapid decryption of quantum computers. The idea behind post-quantum cryptography is that ideally it should take equally long for a classical computer and a quantum computer to crack the key, and should also be incredibly secure against both types of computers.

Within this competition, 69 competitors, cryptography experts and researchers, created new encryption systems to enter the competition, but by the end of the competition, only 4 of these systems were chosen. These 4 were based on lattices and hash functions, and proved to be incredibly quantum-safe, and so are now being used to encrypt incredibly important and sensitive information worldwide, such as financial information and government documents. This is necessary as the worldwide race for quantum computer development is a threat for national security - whoever gets the best computer first is thus able to crack all of this encryption and access secrets. Thankfully, these algorithms seem to function well and will hopefully improve in the future.