My name is Xiaoquan Huang, and this is my video for my project on RSA encryption and decryption algorithms. And here is my program. By inputting a string, this program is able to encrypt a message, output the cipher text, and decrypt the message. Here, if we input the string “This program is amazing!”, we can see the cipher text generated and the decrypted message afterwards. Let’s see what happens if we input the same string again. Even though they are the same string, the cipher texts generated are not the same.

However, this seems perfect encryption algorithm is no match to this machine. A quantum computer. So what is quantum computing? Quantum computing studies theoretical computational systems. It makes direct use of quantum-mechanical phenomena, such as the superposition and entanglement to perform operations on data.

Quantum computing is able to solve certain problems much more quickly. Some of the well known methods are Shor’s algorithm, simulation of quantum many-body systems, Simon’s algorithm etc.

Qbits are units of quantum information. Quantum mechanics allows the qubits to be in a superposition of both states at the same time. The use of Qbits allows for an increase in computing power.

Shor’s algorithm is a prime example of quantum computing. It runs in polynomial time and the factoring of large numbers become easier.

This propose threat to the widely used encryption schemes. The public-key encryption is based on the assumption that the factorization of large numbers is computationally intractable. However, with a quantum computer, one is able to do so in a much more efficient way.

And that is it, thanks for watching.