Quiz 6

學號：110550091　　名字：吳承瑀

1. Shor's Algorithm can be used to do which of the following?
   Ans: (3) Factor very large integers

Shor's Algorithm

- Shor's algorithm shows (in principle,) that a quantum computer is capable of factoring very large numbers in polynomial time.

The algorithm is dependant on

- **Modular Arithmetic**
- Quantum Parallelism
- Quantum Fourier Transform

2. Why would RSA encryption be considered unsafe from quantum algorithms?
   Ans: (2) Its factors can be determined using Shor's Algorithm and
   (4) The key is solved in polynomial time.

Overview

- RSA uses a public key N which is the product of two large prime numbers
- One way to crack RSA encryption is by factoring N, but with classical algorithms, factoring becomes increasingly time-consuming as N grows large; more specifically
- no classical algorithm is known that can factor in polynomial time.
- Shor's algorithm can crack RSA in polynomial time.

3. Why is AES-GCM preferred and the AES-CBC support was removed in TLS1.3?
   Ans: Beast Attack

The Beast Attack

- **BEAST** 全名為 **Browser Exploit Against SSL/TLS**
- 關鍵在於 SSL 3.0 以及 TLS 1.0 以前所使用的 Cipher Block Chain (CBC) 加密模式。
- 並非這個模式本身有問題，而是它們 (SSL 3.0 以及 TLS 1.0 以及它們以前的版本) 的**使用方法的問題**。