

# Quiz 6

- **Shor's Algorithm can be used to do which of the following?**
  1. Create superposition
  2. Create entanglement
  3. Factor very large integers
  4. Increase algorithm time

# Quiz 6

## **2. Why would RSA encryption be considered unsafe from quantum algorithms?**

1. It includes quantum-proof factoring
2. Its factors can be determined using Shor's Algorithm
3. It is an outdated technology, even for traditional computers
4. The key is solved in polynomial time

# Quiz 6

**3. Why is AES-GCM preferred and the AES-CBC support was removed in TLS1.3 ?**