

# Quantum Computing

A quantum computer uses **quantum bits** and relies on of **quantum-mechanical phenomena** to perform computation

1. Brute-forcing n-bits key with Grover's algorithm would take  **$2^{n/2}$** 
  - ➡ Using symmetric encryption is still doable
2. Factoring prime numbers with Shor's algorithm would be done in polynomial time
  - ➡ Using asymmetric encryption is at risk
  - ➡ Problem for key exchange

# Post-quantum Cryptography

Cryptographic schemes that can defeat quantum computers

➡ Still in research (started around 2006)

[https://en.wikipedia.org/wiki/Post-quantum\\_cryptography](https://en.wikipedia.org/wiki/Post-quantum_cryptography)