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 $\mathbf{2^{n/2}}$
   ➡ **Using symmetric encryption is still safe**

2. Factoring prime numbers with Shor's algorithm would be done in polynomial time
   ➡ **Using asymmetric encryption (key exchange and digital signatures) is at risk**

Post-Quantum Cryptography

Cryptographic schemes that can defeat quantum computers

- ➡ Still in research (started around 2006)
- ➡ On August 2024, the NIST released final versions of the first three Post Quantum Crypto Standards
- ➡ On November 2024, the NIST has announced prohibiting classical cryptography (RSA, DSA, ECDSA, ECDH) after 2035