Post-Quantum Cryptography

- **NIST = National Institute of Standards and Technology**
- **Standardizing one or more quantum-resistant public-key cryptographic algorithms**
- **For use on classical computers**
- **Must be resistant to classical and quantum computing attacks**
- **Second-round candidate algorithms include:**
  - **17 public-key encryption and key-establishment algorithms**
  - **9 algorithms for digital signatures**
- **"*A wide range of mathematical ideas are represented by these algorithms… to hedge against the possibility that if someone breaks one, we could still use another.*"**
- **pqcrypto.org - Dan Bernstein's post-quantum cryptography resources**

NIST Post-Quantum-Cryptography-Standardization

NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'