

EN / LEARNING SERIES

Post-Quantum Security Primer

What organizations can responsibly do today

SCIENCE · TECHNOLOGY · TALENT · FUTURE

Independent educational publication. Concepts are presented for learning and should be validated against primary technical sources for research, engineering or security decisions.

1. The risk

A sufficiently capable fault-tolerant quantum computer could use Shor's algorithm against widely used public-key systems such as RSA and elliptic-curve cryptography.

The exact timeline is uncertain. Migration still matters because encrypted information collected today may remain sensitive for many years.

KEY TERMS

Shor's algorithm • RSA • ECC • harvest now decrypt later

2. Cryptographic inventory

Identify where public-key cryptography is used across applications, devices, certificates, identity systems, software supply chains and third parties.

Record algorithms, key sizes, owners, data lifetime and upgrade constraints. The inventory becomes the basis for prioritization.

KEY TERMS

assets • algorithms • owners • data lifetime

3. Crypto-agility and migration

Design systems so algorithms and keys can be replaced without redesigning the entire product. Test standardized post-quantum algorithms in controlled environments and follow authoritative implementation guidance.

Avoid inventing cryptography. Plan interoperability, performance, certificates, hardware support and fallback behavior.

KEY TERMS

crypto-agility • standards • testing • interoperability

4. Ninety-day starter plan

Weeks 1-3: establish ownership and scope. Weeks 4-7: inventory critical systems and long-lived data. Weeks 8-10: classify risk and dependencies. Weeks 11-13: define pilot migrations and procurement requirements.

KEY TERMS

owner • inventory • priorities • pilot

Suggested practice

Use the interactive modules at quantumserbia.com to test the ideas in this guide. Write down a prediction before every simulation, then compare the result and explain any difference.