

OUR LEARNING EXCLUSIVE

- 14 browser-based labs on thinqtanklearning.com — nothing to install
- Genuine post-quantum cryptography in the labs, not screenshots
- Course-specific thinQtank® Learning publications to make the learning fun and engaging
- Extended hours of training, including immersive hands-on exercises
- No vendor test to teach to — every day is hands-on engineering
- All reading material sent to you when you register
- Six months mentoring access to our engineers after the course

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as a **five-day instructor-led training camp**, Monday to Friday, with roughly half lecture and half hands-on lab work. The balance is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

PREREQUISITES

- Security+ level knowledge of cryptography: symmetric and asymmetric ciphers, hashes, PKI and TLS
- Comfort at a Linux command line
- No physics or advanced mathematics required

TARGET AUDIENCE

- Network and security engineers
- PKI, cryptography and identity administrators
- ISSOs, ISSMs and compliance staff facing CNSA 2.0 milestones
- Security architects and CISO staff planning a migration
- DoD, federal and defense-contractor personnel

CERTIFICATE**No vendor exam — thinQtank® Learning certificate of completion**

Awarded on completing the 14 labs and the capstone. The course is built around the published **NIST FIPS 203, 204 and 205** standards and the **NSA CNSA 2.0** transition timeline.

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

EXCLUSIVE LEARNING PACKAGE

- Quantum-Safe Cryptography Course Guide
- Lab guide, with optional "do it for real" steps for any Linux system with OpenSSL 3.5
- Five daily slide decks
- 14 browser-based labs plus the capstone, with access continuing after class
- Interactive BB84, Grover and hybrid-handshake simulators
- Knowledge checks at the end of every module

COURSE OVERVIEW

thinQtank® Learning is offering a unique **five-day training camp** comprised of five days of instructor-led learning that gives students the knowledge and skills needed to understand, assess and migrate to quantum-safe cryptography — from the physics and history of quantum key distribution, through the quantum threat to RSA and elliptic-curve cryptography, to the NIST post-quantum standards that browsers, SSH, VPNs and PKI are adopting today.

Every day is built around hands-on labs that run in the browser on thinqtanklearning.com. Students run real quantum algorithms on a simulator, catch an eavesdropper on a BB84 link, generate genuine ML-KEM, ML-DSA and SLH-DSA keys, build hybrid post-quantum TLS, SSH and IPsec, and finish with a capstone readiness assessment of a simulated defense-contractor network.

There is no vendor certification exam for this subject. Students who complete the labs and the capstone earn the thinQtank® Learning **Quantum-Safe Cryptography certificate of completion**.

WHAT YOU WILL BE ABLE TO DO

- Explain to leadership why quantum computing breaks today's public-key cryptography, and when it matters
- Find and inventory the cryptography an organization depends on, and rank it by quantum risk
- Deploy and verify hybrid post-quantum TLS, SSH and IPsec
- Build and troubleshoot a post-quantum PKI
- Write a migration roadmap aligned to NIST and NSA CNSA 2.0 timelines

COURSE OBJECTIVES

Primary course objectives:

- Identify which classical algorithms depend on factoring and discrete logarithms, and why that matters
- Describe qubits, superposition, measurement, entanglement and the no-cloning theorem without heavy math
- Trace the history of the field, from Wiesner and BB84 to Shor, Grover and the NIST standards
- Quantify the threat from Shor's and Grover's algorithms, harvest-now-decrypt-later, and Mosca's inequality
- Explain QKD protocols (BB84, E91, decoy-state, MDI, CV-QKD), their limits and government positions on them
- Compare the post-quantum math families: lattice, hash-based, code-based, multivariate and isogeny
- Apply the NIST standards: ML-KEM (FIPS 203), ML-DSA (FIPS 204), SLH-DSA (FIPS 205), plus the FN-DSA and HQC work in progress
- Map policy and protocol work: NIST IR 8547, NSA CNSA 2.0, NSM-10, and IETF hybrid key exchange for TLS, SSH and IKEv2
- Recognize where post-quantum cryptography already runs in production today
- Plan migration: crypto inventory and CBOMs, crypto-agility, hybrid deployment, handshake size, PKI and code signing
- Evaluate what's on the horizon: error-corrected quantum hardware, the quantum internet, and new signature schemes

THE FIVE-DAY CAMP

Day 1**Roots**

Classical crypto, quantum mechanics, history

Day 2**Threat & QKD**

Shor, Grover, quantum key distribution

Day 3**PQC math & standards**

Lattices, hashes, codes; FIPS 203–205

Day 4**PQC in production**

TLS, SSH, IPsec, PKI

Day 5**Migration & horizon**

Inventory, roadmap, capstone

COURSE MODULES

01 Classical Crypto Under the Microscope

- › Symmetric ciphers, hashes, Diffie-Hellman, RSA, ECC, PKI and TLS 1.3
- › Which pieces rest on factoring and discrete logarithms

02 Quantum Mechanics for Security People

- › Qubits, superposition, measurement, entanglement, no-cloning, Bell tests

03 History of Quantum Cryptography

- › Conjugate coding, BB84, E91, Shor and Grover
- › The 2022 breaks of SIKE and Rainbow

04 The Quantum Threat Model

- › Shor vs. RSA and ECC; Grover vs. AES and SHA
- › Harvest now, decrypt later; Mosca's inequality

05 Quantum Key Distribution

- › BB84, E91, decoy-state, MDI and continuous-variable QKD; QBER and privacy amplification
- › Trusted-node and satellite networks; QRNGs; limits and government positions

06 Post-Quantum Math Families

- › Lattice, hash-based, code-based, multivariate and isogeny schemes

07 Standards and Policy

- › FIPS 203, 204, 205; FN-DSA and HQC in progress
- › NIST IR 8547, CNSA 2.0, NSM-10; IETF hybrid TLS, SSH and IKEv2

08 Post-Quantum Cryptography in Production

- › Browsers, messaging, OpenSSH, OpenSSL 3.5, cloud KMS and HSMs, Cisco IKEv2

09 Migration Engineering

- › Inventory and CBOMs, crypto-agility, hybrid deployment
- › Handshake size and MTU, PKI and code signing, IoT/OT, vendor questions

10 On the Horizon

- › Error-corrected hardware, the quantum internet, new signature schemes

HANDS-ON LABS

L01 Why factoring matters**L02** Shor's algorithm on a quantum simulator and replayed IBM hardware runs**L03** Grover search vs. AES key strength**L04** BB84 key exchange with an eavesdropper**L05** QKD network design and key-rate limits**L06** Post-quantum toolkit: ML-KEM, ML-DSA and SLH-DSA**L07** Finding post-quantum key exchange in real captures**L08** Building a hybrid post-quantum TLS server**L09** Quantum-safe SSH**L10** Cisco IKEv2 with a post-quantum preshared key**L11** Building a post-quantum PKI**L12** Crypto inventory and CBOM**L13** Walkthrough: how SIKE was broken**L14** Virtual optics bench**CAP** quantum readiness assessment of a simulated defense-contractor network

Every lab runs in the browser on thinqtanklearning.com — nothing to install. Labs 6 and 11 generate genuine ML-KEM, ML-DSA and SLH-DSA keys and signatures. The lab guide adds optional steps to repeat labs 8–12 on any Linux system with OpenSSL 3.5.

COURSE AT A GLANCE

Duration

Five days, Monday to Friday

Lecture / lab

About 50% / 50%

Labs

14 plus capstone, all in the browser

Exam

None — certificate of completion

Delivery

Classroom, live online or on-site

TERMS

© 2026 thinQtank® Global, Inc. All rights reserved. The product or learning materials are protected by U.S. and intellectual property laws. thinQtank Global, thinQtank Learning and the QMan logo are registered trademarks of thinQtank Global, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. thinQtank Global, Inc. warrants that it will perform these training services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY THINQTANK GLOBAL, INC., OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. THINQTANK GLOBAL, INC. WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this training are copyrighted by thinQtank Global, Inc. ("Learning Materials"). thinQtank Global, Inc. grants the customer of this learning a license to use Learning Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of the technology covered herein. Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this training.