Quantum Cryptography and Post-Quantum Security Planning Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The looming threat of fault-tolerant quantum computers necessitates a paradigm shift in global cybersecurity. Current public-key cryptosystems like RSA and ECC, which form the bedrock of digital security for e-commerce, banking, and critical infrastructure, are highly vulnerable to algorithms like Shor's algorithm. Quantum Cryptography and Post-Quantum Security Planning Training Course is specifically designed to equip technical leaders and security professionals with the cutting-edge knowledge required to navigate this quantum transition. It offers a deep dive into Quantum Key Distribution (QKD) leveraging the laws of quantum physics for theoretically unbreakable key exchange and the math-based approach of Post-Quantum Cryptography (PQC), which relies on new, complex mathematical problems resistant to both classical and quantum attacks.

This intensive training focuses on both the theoretical foundations and practical implementation of quantum-safe security. Participants will gain expertise in NIST PQC standardization efforts, cryptographic migration strategies, and the deployment of quantum-resistant algorithms such as lattice-based and hash-based schemes. Mastering these concepts is critical for future-proofing organizational security architectures, ensuring data integrity, and maintaining confidentiality in the face of the emerging quantum threat. Completion of this course will position attendees as subject matter experts ready to develop and execute a robust Post-Quantum Security Plan for their organizations.

Programme Curriculum

Quantum Cryptography and Post-Quantum Security Planning Training Course

Introduction

The looming threat of fault-tolerant quantum computers necessitates a paradigm shift in global cybersecurity. Current public-key cryptosystems like RSA and ECC, which form the bedrock of digital security for e-commerce,

banking, and critical infrastructure, are highly vulnerable to algorithms like Shor's algorithm. Quantum Cryptography and Post-Quantum Security Planning Training Course is specifically designed to equip technical leaders and security professionals with the cutting-edge knowledge required to navigate this quantum transition. It offers a deep dive into Quantum Key Distribution (QKD) leveraging the laws of quantum physics for theoretically unbreakable key exchange and the math-based approach of Post-Quantum Cryptography (PQC), which relies on new, complex mathematical problems resistant to both classical and quantum attacks.

This intensive training focuses on both the theoretical foundations and practical implementation of quantum-safe security. Participants will gain expertise in NIST PQC standardization efforts, cryptographic migration strategies, and the deployment of quantum-resistant algorithms such as lattice-based and hash-based schemes. Mastering these concepts is critical for future-proofing organizational security architectures, ensuring data integrity, and maintaining confidentiality in the face of the emerging quantum threat. Completion of this course will position attendees as subject matter experts ready to develop and execute a robust Post-Quantum Security Plan for their organizations.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Define the fundamental principles of Quantum Computing and its cryptographic implications.
2. Analyze the Quantum Threat Landscape including the impact of Shor's and Grover's algorithms.
3. Differentiate between Quantum Cryptography (QKD) and Post-Quantum Cryptography (PQC).
4. Evaluate the primary categories of PQC Algorithms: lattice-based, hash-based, code-based, and multivariate.
5. Explain the current status and roadmap of the NIST PQC Standardization process.
6. Design a phased, risk-based Cryptographic Migration Strategy for quantum resilience.
7. Implement and test core PQC Schemes using open-source libraries.
8. Assess the performance and resource overhead of Quantum-Resistant Cryptography in enterprise systems.
9. Develop a Cryptographic Inventory Management framework to identify vulnerable assets
10. Formulate a secure Hybrid Cryptosystem combining classical and post-quantum techniques.
11. Analyze QKD Protocols and their deployment in fiber-optic and satellite networks.
12. Integrate Quantum-Safe Security into modern infrastructures like Cloud, 5G, and IoT environments.
13. Construct a comprehensive Post-Quantum Security Planning policy and governance model.

Target Audience

1. Cybersecurity Architects and Engineers
2. Chief Information Security Officers (CISOs) and Security Managers
3. Cryptographers and Security Researchers
4. IT Infrastructure and Cloud Security Professionals
5. Software Developers and Application Security Specialists
6. Government and Defense Technology Strategists
7. Risk Management and Compliance Officers in Finance/Healthcare
8. Network Engineers and Telecommunications Specialists

Course Modules

Module 1: The Quantum Threat and Cryptographic Foundations

- Classical Cryptography Review.
- Fundamentals of Quantum Computing.
- The Quantum Attack
- Defining the Threat Horizon.
- Case Study: RSA Vulnerability in Financial Services.

Module 2: Quantum Key Distribution (QKD) Principles

- QKD Mechanics
- Core QKD Protocols.
- QKD Implementation Challenges.
- QKD and PQC
- Case Study: QKD Deployment in Government Networks.

Module 3: Post-Quantum Cryptography (PQC) & NIST Standardization

- Introduction to PQC.
- PQC Categories Overview.
- NIST PQC Process
- Key Exchange and Signature Schemes
- Case Study: PQC Standardization and IP Licensing.

Module 4: Deep Dive into Lattice-Based Cryptography

- Mathematical Foundations.
- Lattice-Based KEMs
- Lattice-Based Digital Signatures.
- Performance Metrics.
- Case Study: Securing IoT Devices with Lattice-Based PQC.

Module 5: Migration and Cryptographic Agility

- The Quantum Risk Assessment.
- Phased Migration Strategy
- Hybrid Mode Implementation.
- Cryptographic Agility.
- Case Study: Global Bank's PQC Transition.

Module 6: PQC Implementation and Testing

- Practical Coding Labs
- Integration with Protocols.
- Post-Quantum Key Management.
- Testing and Validation.
- Case Study: Implementing PQC in a Cloud HSM.

Module 7: Quantum-Safe Enterprise Security Architectures

- Cloud Security.
- Network and 5G Security.

- IoT and Embedded Systems.
- Code-Based and Hash-Based Signatures.
- Case Study: Securing the Energy Grid.

Module 8: Policy, Governance, and the Quantum Future

- Developing a Post-Quantum Security Policy.
- Legal and Regulatory Compliance
- Future of Quantum Internet.
- Emerging Cryptographic Research.
- Case Study: National Post-Quantum Roadmap.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com