Quantum Computing and its Impact on Cryptography Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Quantum computing is rapidly emerging as a disruptive force with the potential to transform modern cryptography, cybersecurity frameworks, and digital privacy infrastructures. As quantum processors grow in speed and capability, traditional encryption methods such as RSA, ECC, and Diffie-Hellman face unprecedented vulnerabilities, requiring organizations to prepare for the shift toward post-quantum cryptography. Quantum Computing and its Impact on Cryptography Training Course equips participants with the foundational understanding of quantum algorithms, cryptographic risks, defensive strategies, and transition planning necessary to navigate the future landscape of secure digital systems.

Through practical analysis, scenario-based discussions, and case-driven exploration, participants will develop the capability to evaluate algorithmic threats, assess quantum resilience, and implement post-quantum readiness plans. The course blends theoretical insights with real-world applications, enabling learners to understand how quantum breakthroughs reshape data protection, regulatory compliance, financial system security, and national digital security strategies. By the end of the program, participants will be prepared to support organizations in securing infrastructures against quantum-enabled attacks and contribute to long-term cryptographic resilience.

Programme Curriculum

Quantum Computing and its Impact on Cryptography Training Course

Introduction

Quantum computing is rapidly emerging as a disruptive force with the potential to transform modern cryptography, cybersecurity frameworks, and digital privacy infrastructures. As quantum processors grow in speed and capability, traditional encryption methods such as RSA, ECC, and Diffie-Hellman face unprecedented vulnerabilities, requiring organizations to prepare for the shift toward post-quantum

cryptography. Quantum Computing and its Impact on Cryptography Training Course equips participants with the foundational understanding of quantum algorithms, cryptographic risks, defensive strategies, and transition planning necessary to navigate the future landscape of secure digital systems.

Through practical analysis, scenario-based discussions, and case-driven exploration, participants will develop the capability to evaluate algorithmic threats, assess quantum resilience, and implement post-quantum readiness plans. The course blends theoretical insights with real-world applications, enabling learners to understand how quantum breakthroughs reshape data protection, regulatory compliance, financial system security, and national digital security strategies. By the end of the program, participants will be prepared to support organizations in securing infrastructures against quantum-enabled attacks and contribute to long-term cryptographic resilience.

Course Objectives

1. Understand fundamental concepts of quantum computing and quantum mechanics.
2. Analyze the vulnerabilities of traditional cryptographic systems to quantum attacks.
3. Evaluate the implications of Shor's and Grover's algorithms on digital security.
4. Assess organizational risks arising from quantum-enabled threats.
5. Understand global trends in post-quantum cryptography and emerging standards.
6. Apply techniques for cryptographic migration and transition planning.
7. Identify secure key management practices in quantum-resistant environments.
8. Examine regulatory and compliance requirements related to quantum security.
9. Explore quantum-safe encryption algorithms and implementation frameworks.
10. Strengthen cybersecurity strategies to align with quantum risk mitigation.
11. Analyze quantum-resistant architectures used in financial and governmental systems.
12. Utilize risk assessment tools for evaluating quantum vulnerabilities.
13. Develop long-term organizational roadmaps for post-quantum readiness.

Organizational Benefits

- Enhanced preparedness for quantum-induced cyber threats
- Strengthened protection of sensitive digital assets
- Improved compliance with emerging post-quantum regulatory standards
- Increased resilience in critical infrastructure environments
- Better alignment of cybersecurity strategy with future technological trends
- Reduced risk of cryptographic failures or data breaches
- Streamlined migration to quantum-safe systems
- Enhanced institutional capacity in encryption management
- Greater competitiveness in digitally transforming industries
- Improved long-term security planning and strategic decision-making

Target Audiences

- Cybersecurity professionals and IT security managers
- Cryptography engineers and encryption specialists
- Government cybersecurity and intelligence units
- Financial sector IT and risk management teams
- Digital transformation and technology innovation leaders
- Compliance officers and regulatory analysts
- Academic researchers and technology strategists

- Telecommunications and infrastructure security teams

Course Duration: 10 days

Course Modules

Module 1: Introduction to Quantum Computing

- Explore quantum mechanics principles relevant to computing
- Understand qubits, superposition and entanglement
- Compare classical and quantum computational models
- Examine quantum hardware and processor evolution
- Identify industries most affected by quantum breakthroughs
- Case Study: Global race in quantum processor development

Module 2: Quantum Algorithms and Cryptographic Implications

- Analyze core quantum algorithms powering computation
- Examine Shor's algorithm and its impact on encryption
- Explore Grover's algorithm and search acceleration risks
- Identify which cryptographic systems face compromise
- Map vulnerabilities across institutional systems
- Case Study: Predicting algorithmic attacks in financial systems

Module 3: Classical Cryptography Under Quantum Threat

- Review RSA, ECC, symmetric encryption and hashing
- Assess quantum exposure points in current cryptographic models
- Understand quantum decryption timelines
- Evaluate long-term confidentiality risks
- Identify processes requiring urgent upgrades
- Case Study: Encryption breakdown in simulated MFI environment

Module 4: Post-Quantum Cryptography Fundamentals

- Review emerging quantum-resistant encryption families
- Understand lattice-based, multivariate, and hash-based algorithms
- Explore NIST's post-quantum cryptography standardization
- Evaluate algorithm performance and implementation needs
- Map integration into current infrastructures
- Case Study: PQC adoption roadmap for a national bank

Module 5: Quantum Key Distribution (QKD)

- Understand principles of QKD and secure photon exchange
- Assess advantages and limitations of QKD networks
- Explore use cases in telecom and financial sectors
- Compare QKD to classical key exchange
- Analyze integration requirements for institutions
- Case Study: Implementation of QKD in a major telecom provider

Module 6: Quantum-Resistant Network Security

- Assess network vulnerabilities to quantum attacks
- Strengthen endpoint protection and secure communications
- Develop hybrid encryption strategies
- Implement layered quantum-defense models
- Evaluate enterprise network readiness
- Case Study: Network redesign under quantum risk assessment

Module 7: Quantum Threat Modelling

- Identify quantum threats to organizational systems
- Map threat vectors in digital identity and data assets
- Use quantum-oriented risk modelling tools
- Prioritize systems based on vulnerability tiers
- Integrate quantum risks into cybersecurity governance
- Case Study: Threat modelling for financial clearing systems

Module 8: Cryptographic Migration Strategies

- Evaluate readiness for cryptographic transition
- Develop migration timelines and sequencing
- Identify performance impacts and implementation risks
- Establish governance structures for migration
- Plan for interoperability and backward compatibility
- Case Study: Migration strategy for a national tax authority

Module 9: Regulatory and Compliance Considerations

- Examine emerging global quantum security regulations
- Review sector-specific compliance requirements
- Align encryption policies with regulatory standards
- Document risk assessments and compliance audits
- Prepare institutions for regulatory inspections
- Case Study: Compliance audit in a cross-border digital platform

Module 10: Quantum Security in Financial Systems

- Investigate quantum risk exposure in payment systems
- Strengthen digital banking and mobile platforms
- Protect financial messaging and transaction networks
- Integrate PQC into digital lending and credit scoring
- Build resilience into fintech and microfinance systems
- Case Study: Quantum-resilient architecture in a central bank

Module 11: Cloud Security and Quantum Risks

- Evaluate cloud vulnerabilities to quantum decryption
- Explore PQC integration in cloud security protocols
- Assess vendor readiness for quantum-safe infrastructure
- Secure cloud-based data storage with future-proof encryption
- Review hybrid and multi-cloud compliance risks
- Case Study: PQC in a cloud-hosted enterprise system

Module 12: Data Protection and Privacy in a Quantum Era

- Assess risks to long-term confidentiality of stored data
- Protect personal data from harvest-now-decrypt-later attacks
- Strengthen secure data retention strategies
- Implement enhanced privacy-preserving techniques
- Align practices with global privacy laws
- Case Study: Data privacy upgrade for a healthcare institution

Module 13: Quantum Computing in Cyber Offense and Defense

- Review quantum-enhanced cyberattack capabilities
- Explore defense strategies leveraging quantum technology
- Strengthen institutional resilience to rapid cryptographic shifts
- Apply simulation tools to test defense mechanisms
- Understand government and military applications
- Case Study: Defensive quantum strategy in critical infrastructure

Module 14: Organizational Preparedness for Quantum Transformation

- Conduct organizational readiness assessments
- Build internal skills and capacity for PQC integration
- Train teams on future cryptographic protocols
- Establish governance frameworks for quantum adoption
- Develop long-term investment strategies
- Case Study: Enterprise-wide PQC readiness assessment

Module 15: Building a Post-Quantum Security Roadmap

- Develop multi-year quantum security strategies
- Prioritize systems for upgrade and testing
- Allocate resources for pilots, testing and deployment
- Build partnerships with technology vendors and regulators
- Enhance monitoring, reporting and system evaluation
- Case Study: National roadmap for post-quantum secure communication

Training Methodology

- Instructor-led expert presentations
- Case study analysis and scenario-based learning
- Group work and peer-learning discussions
- Hands-on exercises using cryptographic tools
- Practical simulations of quantum threat models
- Development of institutional action plans

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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