COURSE TABLE OF CONTENTS

# Post-Quantum Cryptography Fundamentals

OEM: Koenig Original • Duration: 3 Days (24 hrs)

## COURSE MODULES & TOPICS

### Module 1: Quantum Computing Fundamentals

- Evolution of quantum computing
- Classical vs quantum computing
- Quantum physics basics for computing
- Qubits and their representation
- Quantum superposition and measurement
- Quantum entanglement and interference

### Module 2: Quantum Circuits and Algorithms

- Quantum gates: Pauli-X, Y, Z, Hadamard, CNOT, controlled gates
- Quantum circuits and their representation
- Quantum registers and multi-qubit systems
- Introduction to quantum algorithms
- Deutsch-Jozsa, Grover's, and Shor's algorithms

### Module 3: Quantum Programming and Simulation

- Quantum computing simulators and frameworks
- Python-based quantum programming with Qiskit
- Quantum circuit simulation using Qiskit Aer

### Module 4: Classical Cryptography Overview

- Introduction to classical cryptography and information security
- Encryption, decryption, hashing, digital signatures
- Symmetric cryptography: AES, ChaCha20
- Asymmetric cryptography: RSA, ECC
- Public key infrastructure, digital certificates, key exchange

### Module 5: Quantum Threats to Cryptography

- Quantum threats against conventional cryptography
- Impact of quantum computing on modern cryptography
- Shor's algorithm vs RSA and ECC
- Grover's algorithm vs symmetric encryption and hash functions
- Quantum attacks vs classical attacks
- Harvest Now, Decrypt Later (HNDL) attacks

### Module 6: Introduction to Post-Quantum Cryptography

- Post-Quantum Cryptography (PQC) overview
- PQC vs Quantum Key Distribution (QKD)
- Objectives and requirements of quantum-resistant algorithms
- Mathematical foundations of PQC

© Koenig Solutions

### Module 7: Post-Quantum Cryptographic Algorithms

- Lattice-based cryptography fundamentals
- Learning With Errors (LWE) and Module LWE
- Hash-based cryptography fundamentals
- Code-based cryptography fundamentals
- Multivariate polynomial-based cryptography
- Isogeny-based cryptography concepts

### Module 8: NIST PQC Standardization and Algorithms

- NIST PQC standardization initiative
- NIST FIPS 203: ML-KEM
- NIST FIPS 204: ML-DSA
- NIST FIPS 205: SLH-DSA
- Security levels and parameter sets

### Module 9: PQC Key Encapsulation and Digital Signatures

- Key Encapsulation Mechanism (KEM): concepts and workflow
- PQC key generation, encapsulation, decapsulation
- Digital signatures using post-quantum algorithms
- Comparison: conventional vs post-quantum algorithms
- Performance: key sizes, signatures, computational overhead

### Module 10: PQC Implementation Frameworks and Tools

- Free and open-source PQC frameworks
- Python-based cryptographic programming
- Open Quantum Safe (OQS) project and ecosystem
- liboqs: architecture, algorithms, capabilities

### Module 11: Implementing PQC Algorithms

- ML-KEM key generation and shared-secret establishment
- Encapsulation and decapsulation with ML-KEM
- ML-DSA key generation and digital signatures
- Signing and verification with ML-DSA
- SLH-DSA and hash-based digital signatures
- Comparative analysis: ML-KEM, ML-DSA, SLH-DSA

### Module 12: Integrating PQC with Existing Systems

- OpenSSL for conventional cryptography
- OpenSSL quantum-safe integration using OQS Provider
- Hybrid cryptography: combining classical and post-quantum algorithms
- Hybrid key exchange: ECC and ML-KEM

### Module 13: Quantum-Safe Communication and Applications

- Post-quantum TLS and quantum-safe communication
- PQC in HTTPS, VPNs, PKI, digital certificates
- PQC in cloud, enterprise, IoT, industrial, financial, government

### Module 14: PQC Migration and Security Assessment

- Cryptographic inventory and quantum-vulnerable algorithm identification
- Quantum readiness assessment and migration planning

- Cryptographic agility and algorithm replacement strategies

### Module 15: Testing, Benchmarking, and Industry Adoption

- Testing and benchmarking PQC implementations
- Comparing RSA/ECC with ML-KEM and ML-DSA
- Security considerations and deployment challenges
- Industry adoption, future developments, emerging standards
- Quantum-safe communication architecture overview

### Module 16: Recommended Tools and Software

- Qiskit and Qiskit Aer for quantum simulation
- Cirq and IBM Quantum Composer
- OpenSSL and PQC support
- liboqs and OQS Provider
- Google Colab for cloud-based Python
- Wireshark for network and TLS analysis