QUANTUM-SAFE CRYPTOGRAPHY LAB SERIES

Lab 1: Kyber Key Exchange with Qiskit

Understanding Post-Quantum Encryption

PART 1: LAB PREPARATION & BACKGROUND

Student Name: _____
Date: _____
Quantum Level: Intermediate-Advanced
Prerequisites: Basic Python, Quantum Superposition, Public-Key Cryptography

---

PRE-LAB QUESTIONS: CRYPTOGRAPHY FUNDAMENTALS

Instructions: Before starting the lab, answer these foundational questions:

1. Public-Key Cryptography: How does RSA encryption work? Why is it vulnerable to quantum computers?

   ---

2. Lattice-Based Cryptography: What mathematical problem makes lattice-based encryption quantum-resistant?

   ---

3. Kyber Specification: Kyber is a CRYSTALS-Kyber MLWE-based KEM. What does MLWE stand for and why is it hard for both classical and quantum computers?

PART 2: THEORETICAL BACKGROUND

Why Kyber? The NIST Standard for Post-Quantum Cryptography

In 2022, the National Institute of Standards and Technology (NIST) selected CRYSTALS-Kyber as the standard for post-quantum public-key encryption. This marked a historic shift from RSA/ECC to quantum-resistant algorithms.

The Quantum Threat Timeline:

- 1994: Peter Shor's algorithm shows quantum computers can break RSA
- 2016: NIST begins post-quantum cryptography standardization
- 2022: Kyber selected as primary KEM (Key Encapsulation Mechanism)
- 2030+: Quantum computers may break current encryption

How Kyber Works:
Kyber is based on the Module Learning With Errors (MLWE) problem. In simple terms:

1. Key Generation: Create public key (matrix A, vector t) and private key (secret s)
2. Encapsulation: Encrypt a symmetric key using public key
3. Decapsulation: Decrypt using private key

The security relies on the difficulty of solving noisy linear equations over lattices—a problem believed to be hard for both classical and quantum computers.

Qiskit's Role:
While Qiskit is primarily for quantum computing, it provides quantum-safe cryptography tools to:

1. Demonstrate why current encryption is vulnerable
2. Implement and test post-quantum alternatives
3. Simulate quantum attacks on classical crypto

PART 3: LAB SETUP & INSTALLATION

Check labs folder at github repository >> https://github.com/learningdungeon/qamp-2025

Step 1: Environment Setup

Step 2: Import Required Libraries

Step 3: Kyber Simulation Functions

(Since full Kyber requires extensive implementation, we'll simulate key components)

PART 4: LAB EXERCISES

Check lab folder at github repository >> https://github.com/learningdungeon/qamp-2025

Exercise 1: Key Generation and Exchange

Practice at the lab and write..

Your Answers:

1. _____
2. _____
3. _____

Exercise 2: Quantum Vulnerability Demonstration

Practice at the lab and write…

Your Answers:
4. _____
5. _____
6. _____

Exercise 3: Implementing Key Exchange Protocol

Practice at the lab and write…

Your Answers:
7. _____
8. _____
9._____

Exercise 4: Security Analysis & Quantum Attack Simulation

Practice at the lab and write…

Your Answers:
10. _____
11. _____
12. _____

PART 5: LAB REPORT & ANALYSIS

Report Questions:

A. Technical Analysis:

1. Describe the complete flow of Kyber key exchange in your own words.

   _____

   _____

2. What is the role of the error terms (e, e1, e2) in Kyber's security?

3. How does Qiskit help in understanding post-quantum cryptography?

B. Comparative Analysis:

4. Create a table comparing RSA, ECC, and Kyber:

Feature	RSA-2048	ECC-256	Kyber-512
Public Key Size			
Security vs Quantum			
Key Exchange Speed			
NIST Status			

C. Quantum Implications:

5. If a quantum computer with 1 million qubits existed today, which current encryption would break first and why?

6. How should organizations prepare for the quantum transition?

D. Implementation Challenge:

7. Propose an enhancement to our simulated Kyber for better security or performance:

PART 6: EXTENSION ACTIVITIES

Check lab folder at github repository >> https://github.com/learningdungeon/qamp-2025

Challenge 1: Implement Real Kyber

Challenge 2: Quantum Network Simulation

Challenge 3: Performance Analysis

PART 7: RESOURCES & REFERENCES

Essential Reading:

1. NIST PQC Standardization: https://csrc.nist.gov/projects/post-quantum-cryptography
2. CRYSTALS-Kyber Specification: https://pq-crystals.org/kyber/

3. Qiskit Textbook - Cryptography: https://qiskit.org/textbook/ch-algorithms/shor.html
4. Python Cryptography Toolkit: https://cryptography.io/

Video Resources:

1. NIST PQC Conference 2023: https://www.youtube.com/watch?v=5OD8A2g6f-I
2. Kyber Deep Dive: https://www.youtube.com/watch?v=UkV9cM-7jYk
3. Quantum Cryptography with Qiskit: https://www.youtube.com/watch?v=8U_6ehyNbvQ

Further Exploration:

1. Implement side-channel attack resistance
2. Study other PQC finalists (Dilithium, Falcon)
3. Explore hybrid schemes (PQC + traditional)
4. Research lattice cryptography mathematics

GRADING RUBRIC

Category	Excellent (4)	Good (3)	Satisfactory (2)	Needs Work (1)
Code Implementation	All exercises completed, runs without errors	Most exercises completed, minor issues	Basic functionality working	Significant errors or missing parts

Concept Understanding	Demonstrates deep understanding of Kyber and quantum threats	Good understanding of key concepts	Basic comprehension	Major misconceptions
Analysis & Reporting	Thorough analysis, clear comparisons, insightful conclusions	Good analysis with most questions answered	Basic answers provided	Incomplete or unclear analysis
Extension Work	Attempted challenges with good results	Attempted at least one challenge	Considered extensions	No extension work
Lab Questions	All questions answered correctly and thoroughly	Most questions answered correctly	Basic answers to main questions	Many questions incomplete

Total Points: _____ / 20
Grade: _____

TEACHER'S NOTES

Lab Setup Requirements:

1. Python 3.8+ with Jupyter Notebook or Google Colab
2. Install: `pip install qiskit cryptography numpy matplotlib`
3. For advanced: `pip install pqcrypto` (real Kyber implementation)

Time Management:

- Basic: Exercises 1-2 (90 minutes)
- Standard: Exercises 1-3 (120 minutes)
- Advanced: All exercises + extensions (180 minutes)

Common Student Challenges:

1. Lattice math complexity - Focus on conceptual understanding over mathematical details
2. Quantum vs post-quantum confusion - Emphasize: quantum computers break some crypto, post-quantum crypto resists this
3. Implementation vs simulation - Clarify this is educational simulation, not production code

Assessment Options:

1. Lab report (Part 5 questions)
2. Code submission with comments
3. Presentation on quantum threats and defenses
4. Research paper comparing PQC algorithms

Real-World Connections:

- Current Events: NIST standards adoption timeline
- Industry: Cloud providers (AWS, Google) already offering PQC
- Government: NSA's CNSA 2.0 timeline for PQC migration
- Research: Ongoing cryptanalysis of Kyber and other PQC

Differentiation Strategies:

- Beginner: Focus on Exercise 1, use provided code as-is
- Intermediate: Modify parameters, analyze security trade-offs
- Advanced: Implement real Kyber, compare with other PQC algorithms
- Research: Investigate side-channel attacks on lattice crypto