Computer Science Department
University of Crete

CS458: Introduction to Cryptography
Project: Transition Framework for PQC

Deadline: 31/01/2024, 23:59

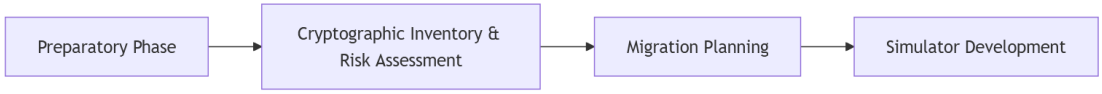
Notes: You will have approximately **2 months** to complete the project. There will be **no extension**. The project accounts for **30%** of the overall grade. It can be done in **teams of up to 4 people**. You are allowed to use **AI tools** or code found online to build a complete system. At the end, there will be an **oral examination** and similarity checking. Due to the workload required, you should **start early** on the necessary research as well as the development.

Introduction

The rise of quantum computing presents a critical challenge to existing cryptographic systems. This project focuses on building a **crypto agility framework** designed to facilitate seamless transition of Post-Quantum Cryptography (PQC) algorithms into existing infrastructures. Through this project, students will:

1. Develop an understanding of cryptographic agility
2. Conduct cryptographic inventory scans
3. Risk assess and prioritize quantum-vulnerable systems
4. Demonstrate PQC transition strategies
5. Design and implement a crypto agility simulation
6. Review standards and guidelines to ensure interoperability and compliance
7. Develop a phased migration roadmap

Project Structure



Part 1: Preparatory Phase (Week 1–2)

- **Goal**: Understand the basics of PQC and cryptographic agility.
- **Tasks**:
  - Study preparatory material (NIST guidelines, PQC Migration Handbook)
  - Identify quantum-vulnerable cryptographic primitives
  - Familiarize with tools and compliance standards
- **Deliverables**:
  - A chapter in your report summarizing initial findings and key terms

Part 2: Cryptographic Inventory and Risk Assessment (Week 3–4)

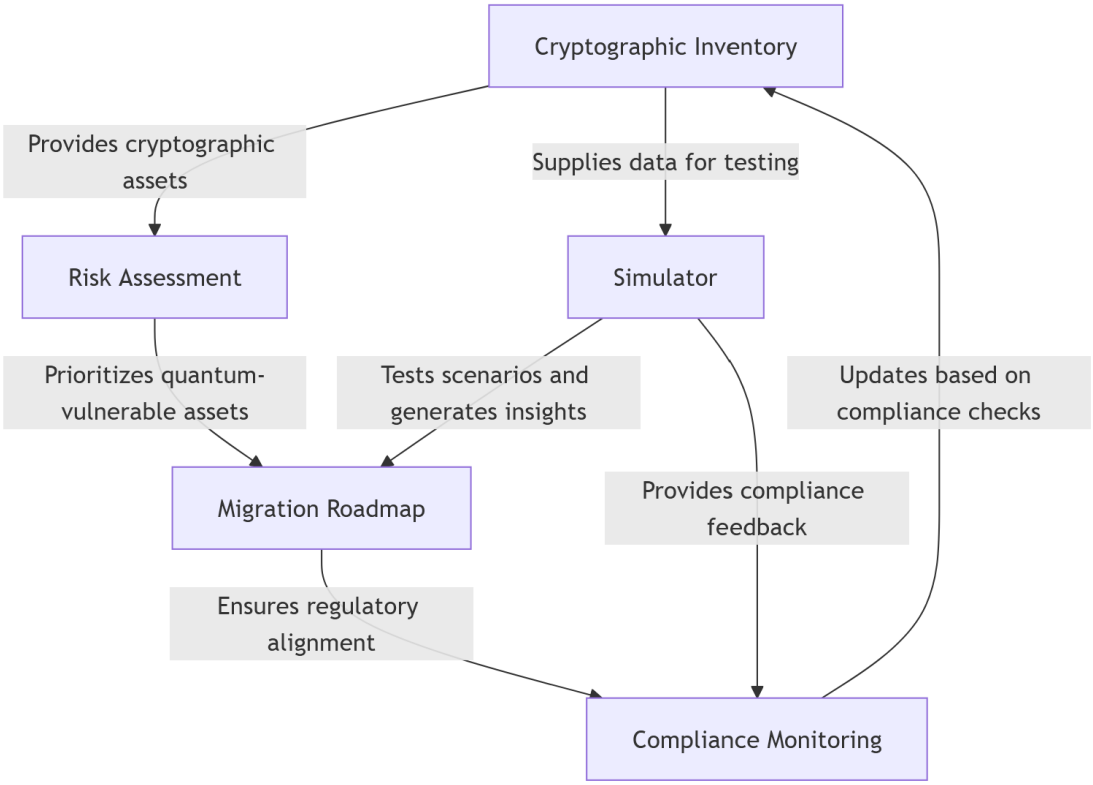
- **Goal**: Build a tool to identify and prioritize quantum-vulnerable assets
- **Tasks**:
  - Develop a database or software to track cryptographic assets
  - Implement a risk assessment module using prioritization algorithms
- **Deliverables**:
  - A working cryptographic inventory tool with a demonstration video
  - A chapter in your report summarizing findings

Part 3: Migration Planning (Week 5–6)

- **Goal**: Create a phased roadmap for PQC transition
- **Tasks**:
  - Design a step-by-step migration plan
  - Include considerations for business continuity and interoperability
- **Deliverables**:
  - A chapter in your report summarizing a migration roadmap with example use cases (e.g., an SME)

Part 4: Simulator Development (Week 7–8)

- **Goal**: Develop a simulator to test PQC transition strategies
- **Tasks**:
  - Simulate quantum-vulnerable systems and transition scenarios
  - Include risk prioritization and compliance monitoring in the simulation
  - Conduct a case study simulating PQC adoption in an SME environment
- **Deliverables**:
  - A functional simulator with a user guide
  - A chapter in your report will be the simulator's user guide
  - A chapter in your report discussing the case study



Output

1. **Report**: Detailed documentation, as described above
2. **Presentation**: Summary of the project for oral defense
3. **Software**: Inventory tool, simulator

Indicative Timetable & Rubric

Week	Phase	Criteria	Weight (%)	Description
1 - 2	**Preparatory Phase**	Initial Understanding	5	Demonstrates understanding of cryptographic agility and PQC fundamentals
		Research Quality	5	Includes well-documented findings from preparatory readings.
3 - 4	**Crypto Inventory & Assessment**	Tool Functionality	25	Accurate and functional inventory tool that identifies and tracks assets
		Risk Prioritization	5	Clear, logical, and correct prioritization of quantum-vulnerable assets
5 - 6	**Migration Planning**	Roadmap Clarity	5	Well-structured, actionable, and realistic migration roadmap
		Business Continuity	5	Considers operational and business priorities during migration
7 - 8	**Simulator Development**	Simulation Accuracy	25	Valid representation of PQC transition scenarios and risk assessments
		User Guide Quality	5	Clear and practical instructions for using the simulator
9 - 10	**Case Study**	Case Study Insights	10	Comprehensive case study report with real-world applicability.
	Overall	Presentation Quality	5	Effective communication of the project through presentations and reports.
		Team Collaboration	5	Evidence of teamwork and fair distribution of tasks.
			100	

Instructions on How AI Tools Can Help

AI tools can greatly enhance efficiency and creativity in this project. Here are phase-specific instructions:

Preparatory phase

- **Literature review**: Use AI tools (e.g., ChatGPT or similar) to summarize key points from NIST guidelines, the PQC Migration Handbook, and other standards
- **Understanding concepts**: Ask AI for clarifications on terms like cryptographic agility, quantum-safe algorithms, and interoperability

Inventory & Assessment

- **Code suggestions**: Use AI coding assistants like GitHub Copilot or ChatGPT to write functions for asset identification and tracking
- **Risk analysis**: Generate risk matrices or models based on inputs, such as asset vulnerabilities and threat levels

Migration Planning

- **Roadmap creation**: Seek AI input for drafting migration phases and aligning them with business continuity goals
- **Document formatting**: Automate the creation of professional-looking documents for the roadmap using templates or AI-based tools

Simulator Development & Case Study

- **Scenario modeling**: Use AI to simulate system responses to quantum threats and develop interactive scenarios
- **Debugging**: Leverage AI to troubleshoot simulation code and suggest optimizations
- **Case study analysis**: Use AI to draft sections of the case study, including cost breakdowns and impact analyses, based on your inputs

General use

- **Collaboration tools**: Utilize AI for task delegation, tracking progress, and maintaining team communication.
- **Presentation preparation**: Create slide content or draft talking points for the final presentation.
- **Code checking**: Validate or optimize code using AI tools for enhanced efficiency.

Guidelines for ethical use of AI

1. **Transparency**: Always cite AI-generated content, whether text, code, or visualizations.
2. **Supplement, not replace**: Use AI as a helper but ensure original understanding and critical thinking.
3. **Plagiarism check**: Run all AI-generated content through plagiarism tools to ensure originality.
4. **Collaboration**: Share AI findings within the team to foster mutual learning and avoid over-reliance by individuals

References

- Wikipedia
  - https://en.wikipedia.org/wiki/Cryptographic_agility
  - https://en.wikipedia.org/wiki/Harvest_now,_decrypt_later
  - https://en.wikipedia.org/wiki/Post-quantum_cryptography
  - https://en.wikipedia.org/wiki/Cryptographic_primitive
- Cryptosense, Cryptographic Inventory
  - https://www.youtube.com/watch?v=91dMLnCv5hQ&list=PLA-8aGQm6tkL6PPTbdg6cy74x7TWFFU3V&ab_channel=Cryptosense (6 short videos)
  - https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWP0kj
- Cryptographic Agility
  - https://www.youtube.com/watch?v=8pGJVTekDyM&ab_channel=RSAConference

- Guidelines
  - …