Computer Science Department
University of Crete

CS458: Introduction to Cryptography
Project: Crypto Agility Framework for PQC

Deadline: 31/01/2025, 23:59
v0.2

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. Ensure you **fully understand all the concepts** involved and **design the architecture properly** before starting to write code.

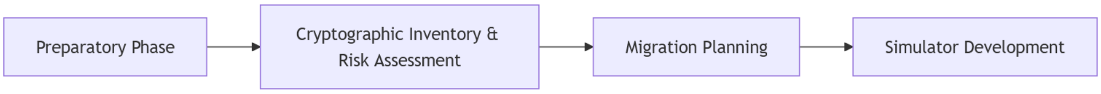
Introduction

The rise of quantum computing presents a critical challenge to existing cryptographic systems[1]. This project focuses on building a **crypto agility[2] framework** designed to facilitate transition from cryptographically vulnerable to cryptographically strong primitives[3]. That includes the transition of Post-Quantum Cryptography[4] (PQC) algorithms into existing infrastructures. Through this project, students will:

1. Develop an understanding of cryptographic agility
2. Design and **implement** a scanner to compile a cryptographic inventory[5]
3. Risk assess[6] and prioritize cryptography-related vulnerable primitives (not just quantum-vulnerable)
4. Review standards and guidelines to ensure interoperability[7] and compliance[8]
5. Develop a phased migration roadmap[9]
6. Demonstrate vulnerable cryptography and PQC transition strategies
7. Design and **implement** a crypto agility simulation

[1] https://en.wikipedia.org/wiki/Harvest_now,_decrypt_later
[2] https://en.wikipedia.org/wiki/Cryptographic_agility
[3] https://en.wikipedia.org/wiki/Cryptographic_primitive
[4] https://en.wikipedia.org/wiki/Post-quantum_cryptography
[5] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWP0kj
[6] https://en.wikipedia.org/wiki/Information_security_management
[7] https://en.wikipedia.org/wiki/Interoperability
[8] https://nordlayer.com/learn/regulatory-compliance/cybersecurity-compliance/
[9] https://en.wikipedia.org/wiki/Technology_roadmap

Project Structure



Part 1: Preparatory Phase (Week 1–2)

- **Goal**: Understand the basics of cryptographic agility, cryptographic inventories and PQC.
- **Tasks**:
  - Study preparatory material
    - Terminology and concepts
    - NIST guidelines[10], European guidelines[11], PQC Migration Handbook[12]
  - Identify vulnerable cryptographic primitives (not just quantum-vulnerable)
  - Familiarize with existing open-source crypto inventory tools
  - Familiarize with existing open-source crypto agility tools
  - Familiarize with compliance standards
- **Deliverables**:
  - A chapter in your report summarizing Part 1 findings and key terms/concepts

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

- **Goal**: **Implement** a tool to identify and prioritize vulnerable crypto primitives
- **Tasks**:
  - Develop software (with a database and GUI) to track cryptographic assets, for example:
    - Target a folder with source code files (e.g., Python files)
    - Search for library calls including weak primitives (e.g., DES, 3DES, AES with weak modes, RSA with short keys, hashes with short lengths, etc.)
  - Implement a risk assessment module that compares your findings to currently accepted best practices
    - Prioritize your findings in terms of criticality
- **Deliverables**:
  - A working **cryptographic inventory tool** with a risk assessment component
  - A chapter in your report summarizing Part 2 findings

[10] NIST, Migration to Post-Quantum Cryptography fact sheet, Aug 2023, https://www.nccoe.nist.gov/sites/default/files/2023-08/quantum-readiness-fact-sheet.pdf

[11] European Commission Recommendation, A Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography, Apr 2024, https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

[12] https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf

Part 3: Migration Planning (Week 5–6)

- **Goal**: Create a phased roadmap for stronger cryptography as well as PQC transition
- **Tasks**:
    - Design a step-by-step migration plan
        - Migration takes time and must be implemented as a structured process
    - Include considerations for business continuity[13] and interoperability and backwards compatibility[14]
- **Deliverables**:
    - A chapter in your report summarizing Part 3 findings (migration roadmap for weak cryptography replacement) with an example use case
        - Use a Small and Medium-Size Enterprise (SME) as a case study
        - Conduct a case study simulating PQC adoption in an SME environment

Part 4: Simulator Development (Week 7–8)

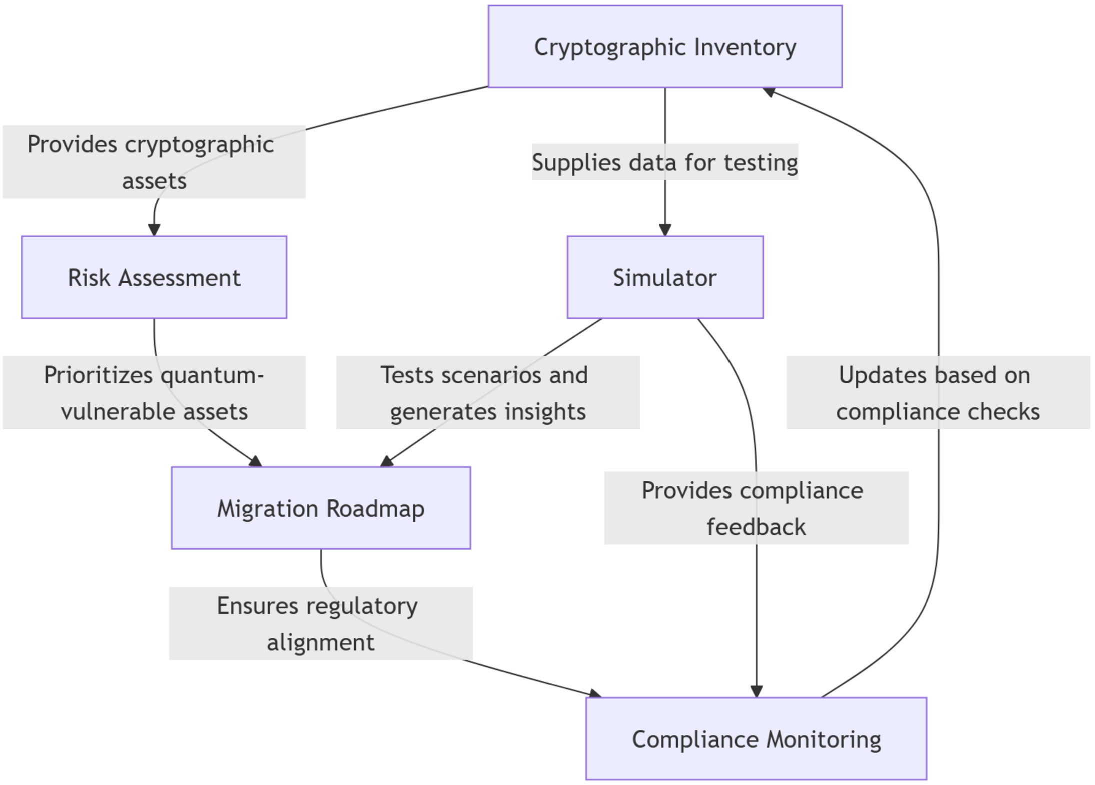
- **Goal**: **Implement** a simulator to demonstrate cryptography transition strategies (for weak cryptography and PQC)
- **Tasks**:
    - Simulate cryptography and quantum-vulnerable systems and transition scenarios
    - Include risk prioritization and compliance monitoring in the simulation
- **Deliverables**:
    - A **functional simulator**
    - A chapter in your report will be the simulator's user guide

Deliverables

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

[13] https://en.wikipedia.org/wiki/Business_continuity_planning

[14] https://en.wikipedia.org/wiki/Backward_compatibility


Cryptographic Inventory
Provides cryptographic assets
Supplies data for testing
Risk Assessment
Simulator
Prioritizes quantum-vulnerable assets
Tests scenarios and generates insights
Updates based on compliance checks
Migration Roadmap
Provides compliance feedback
Ensures regulatory alignment
Compliance Monitoring

Indicative Timetable & Rubric

Week	**Phase**	**Criteria**	**Weight (%)**	**Description**
1 - 2	**Preparatory Phase**	Initial Understanding	5	Demonstrates understanding of cryptographic agility, cryptographic inventory 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 cryptography-related assets
		Risk Prioritization	5	Clear, logical, and correct prioritization of cryptography-vulnerable assets
5 - 6	**Migration Planning & Case Study**	Roadmap Clarity	5	Well-structured, actionable, and realistic migration roadmap
		Business Continuity	5	Consider operational and business priorities during migration (e.g., in an SME environment)

		Case Study Insights	10	Comprehensive case study report with real-world applicability.
7 - 8	**Simulator Development**	Simulation Accuracy	25	Valid representation of cryptography (including PQC) transition scenarios and risk assessments
		User Guide Quality	5	Clear and practical instructions for using the simulator
	Overall	Presentation Quality	5	Effective communication of the project through presentations and reports. Evidence of teamwork and fair distribution of tasks.
		Creativity	5	Evidence of original approaches and problem-solving skills
			100	

Instructions on How AI Tools Can Help

AI tools (ChatGPT, Gemini, Windows copilot, GitHub Copilot, code tools) can greatly enhance **efficiency** and **creativity** in this project. Here are phase-specific instructions:

Preparatory phase

- **Literature review**: Use AI tools to summarize key points from reference web pages, documents and standards
- **Understanding concepts**: Ask AI for clarifications on terms like cryptographic agility, cryptographic inventory, vulnerable cryptographic artifacts, quantum-safe algorithms, interoperability, compliance, transition, roadmap, etc.

Cryptography inventory & Assessment

- **Code suggestions**: Use AI coding assistants to write functions for cryptographic asset identification and tracking, database storage and GUI displays. Generated pseudocode for asset scanning and database integration should be tested and refined for accuracy.
- **Database integration**: Seek AI suggestions for designing and optimizing database schemas to track cryptographic assets.
- **Risk analysis**: Generate risk matrices[15] or models based on inputs, such as asset vulnerabilities and threat[16] levels

Migration Planning & Case Study

- **Roadmap creation**: Seek AI input for drafting migration phases and aligning them with business continuity goals (use an SME as a case study)
- **Visualization**: Create timelines or other visual aids to showcase the plan

[15] https://en.wikipedia.org/wiki/Risk_matrix
[16] https://en.wikipedia.org/wiki/Threat_(computer_security)

- **Case study analysis**: Use AI to draft sections of the case study, potentially including cost breakdowns and impact analyses, based on your inputs

Simulator Development

- **Scenario modeling**: Use AI to help you simulate system responses to weak cryptography threats versus vulnerable assets and develop interactive scenarios. While AI can assist with basic scenario modeling, you must critically evaluate the simulated outputs for correctness.
- **Practical examples/prompts**:
    - "Generate sample datasets for testing quantum-vulnerable cryptographic systems"
    - "Suggest algorithms for automating risk prioritization"

General use

- **Experiment** with various AI tools to identify those best suited to specific phases of the project
- **Collaboration**: You may utilize AI tools for sharing notes, task delegation, tracking progress, and maintaining team communication.
- **Presentation preparation**: Create slide content or draft talking points for the final presentation (e.g., based on the contents of your report as well as the implemented code).
- **Document formatting**: Automate the creation of professional-looking documents (e.g., for the roadmap) using timelines, flowcharts, tables, etc.
- **Debugging**: Leverage AI to troubleshoot crypto inventory and simulation code
- **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. As already stated, there is no penalty for AI use.
2. **Supplement, not replace**: Use AI as a helper but *ensure original understanding and critical thinking.*
3. **Collaboration**: Share AI findings within the team to foster mutual learning and avoid over-reliance by individuals

References

- Cryptosense, Cryptographic Inventory
    - https://www.youtube.com/watch?v=91dMLnCv5hQ&list=PLA-8aGQm6tkL6PPTbdg6cy74x7TWFFU3V&ab_channel=Cryptosense (6 short videos)
- Cryptographic Agility
    - https://www.youtube.com/watch?v=8pGJVTekDyM&ab_channel=RSAConference