Real-Time Use Case: Quantum Computing in Cryptography

Gap Analysis Table

Category : Quantum Algorithms

- **Current Skills Available :** Basic understanding of classical encryption
- **Required Skills :** Knowledge of Shor's and Grover's algorithms
- **Gap identified :** Lack of awareness of quantum threats

Category : Post-Quantum Cryptography (PQC)

- **Current skills Available :** Familiarity with RSA, ECC
- **Required skills:** Understanding lattice-based, hash-based cryptography
- **Gap identified:** No practical exposure to PQC methods

Category : Quantum Programming

- **Current skills Required :** Knows classical programming (C++, Python)
- **Required skills : e**xperience with Qiskit, Cirq, and quantum circuits
- **Gap Identified :** No hands-on quantum coding experience

Category: Implementation & Security

- **Current skills Available :** Standard cryptographic implementations
- **Required Skills :** Securing networks against quantum attacks
- **Gap Identified :** Lack of real-world quantum security solutions

Skills Developed Through Design Thinking

Stage	Skills Developed
Empathize	Understanding cybersecurity risks posed by quantum computing and the industry's preparedness.
Define	Identifying the key areas where skills are lacking, particularly in post-quantum cryptography.
Ideate	Exploring solutions such as online quantum programming courses, PQC workshops, and interactive learning.
Prototype	Developing training modules that focus on quantum cryptography and its real-world applications.
Test	Evaluating effectiveness through hackathons, research projects, and security simulations.