Project Abstract: Exploring Quantum Code-Breaking and its Advantages

Abstract: This project delves into the potential of quantum computing for code-breaking, specifically focusing on its advantages over classical computing methods. We will explore the limitations of classical algorithms like brute force, which exhibit exponential time complexity when dealing with complex encryption schemes.

Focus: Our primary focus will be on **Shor's algorithm**, a powerful quantum algorithm designed to efficiently factor large integers. Factoring large integers forms the foundation for breaking public-key cryptography systems like RSA, which rely on the mathematical difficulty of this task.

Methodology:

1. **Literature review:** We will conduct a comprehensive literature review of relevant research papers and articles to gain a deeper understanding of:
    - Classical code-breaking techniques, including brute force and cryptanalysis.
    - Quantum code-breaking techniques, with a specific emphasis on Shor's algorithm and its theoretical foundation in quantum mechanics concepts like superposition and entanglement.
2. **Simulation:** We will develop a **simulated implementation** of Shor's algorithm using a classical programming language like Python or C++. This simulation will:
    - Utilize **quantum circuit libraries** to represent the quantum operations involved in Shor's algorithm.
    - Simulate the algorithm's execution on a **simulated quantum computer**.
    - Analyze the results to demonstrate the algorithm's ability to factor integers exponentially faster than classical methods for specific key sizes.
3. **Complexity Analysis:** We will perform a comparative analysis of the time complexities of classical and quantum code-breaking algorithms. This analysis will highlight the **exponential speedup** offered by Shor's algorithm, emphasizing the significant advantage it holds over classical approaches for factoring large numbers.

Expected Outcomes:

- Gain a deeper understanding of the theoretical underpinnings of classical and quantum code-breaking algorithms.
- Demonstrate the **computational advantage** of Shor's algorithm over classical methods through a simulated implementation and complexity analysis.
- Raise awareness of the urgency for developing and implementing **post-quantum cryptography (PQC)** to mitigate the threat of quantum attacks on existing encryption schemes.