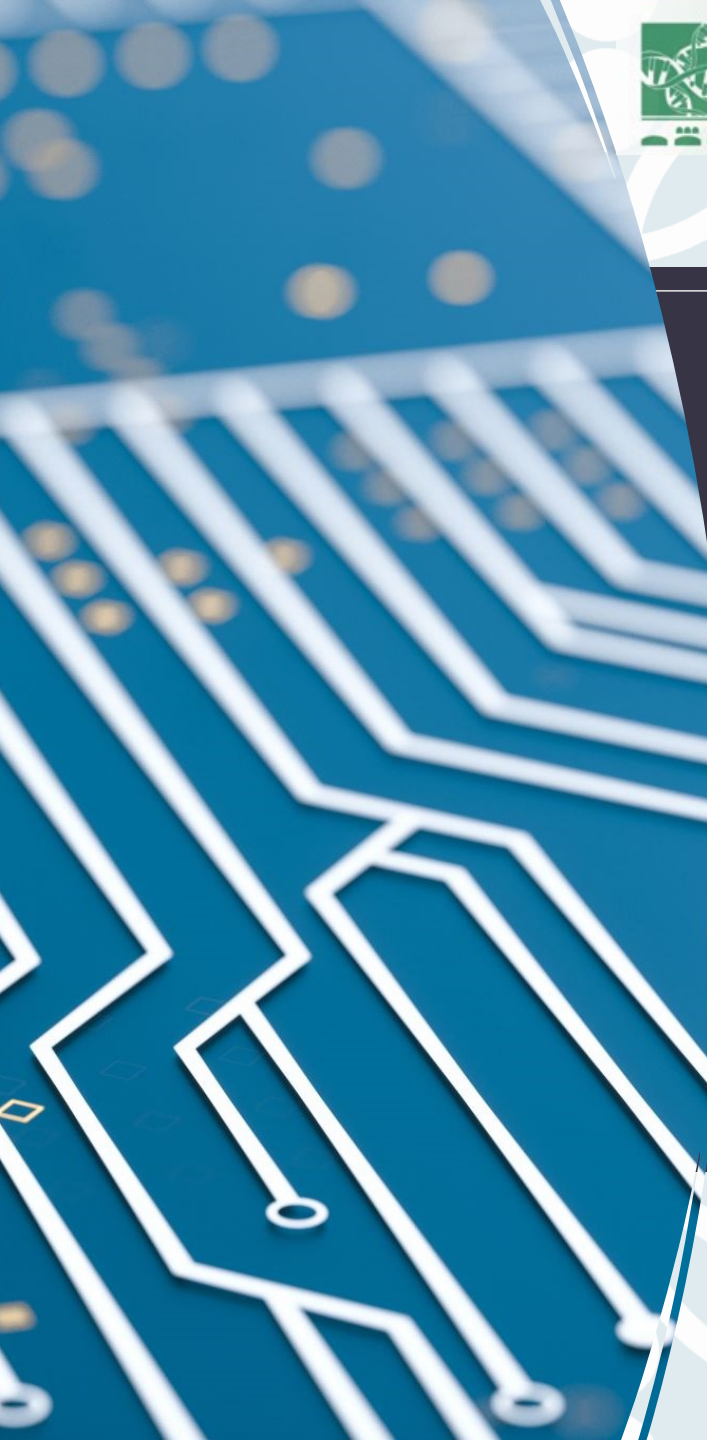
New Perspectives in Science Education
International Conference
NEW PERSPECTIVES in SCIENCE EDUCATION
Edition 15



Designing and Implementing CryptoLearn: A Web-Based Platform for Cryptography and Quantum Computing Education

Sherif Abdelhamid, James Bangura, James Jeffers, Mona Aly

VIRGINIA MILITARY INSTITUTE

Motivation

- Digital society relies on secure communication
- Quantum computing threatens current cryptography
- Cryptography is usually taught late in curricula
- Need accessible, interactive learning tools

Objective

Develop a platform that:

- Introduces cryptography and quantum concepts early
- Uses simple explanations and visual illustrations
- Provides interactive exercises with feedback
- Integrates game-based learning
- Supports scalability and extensibility

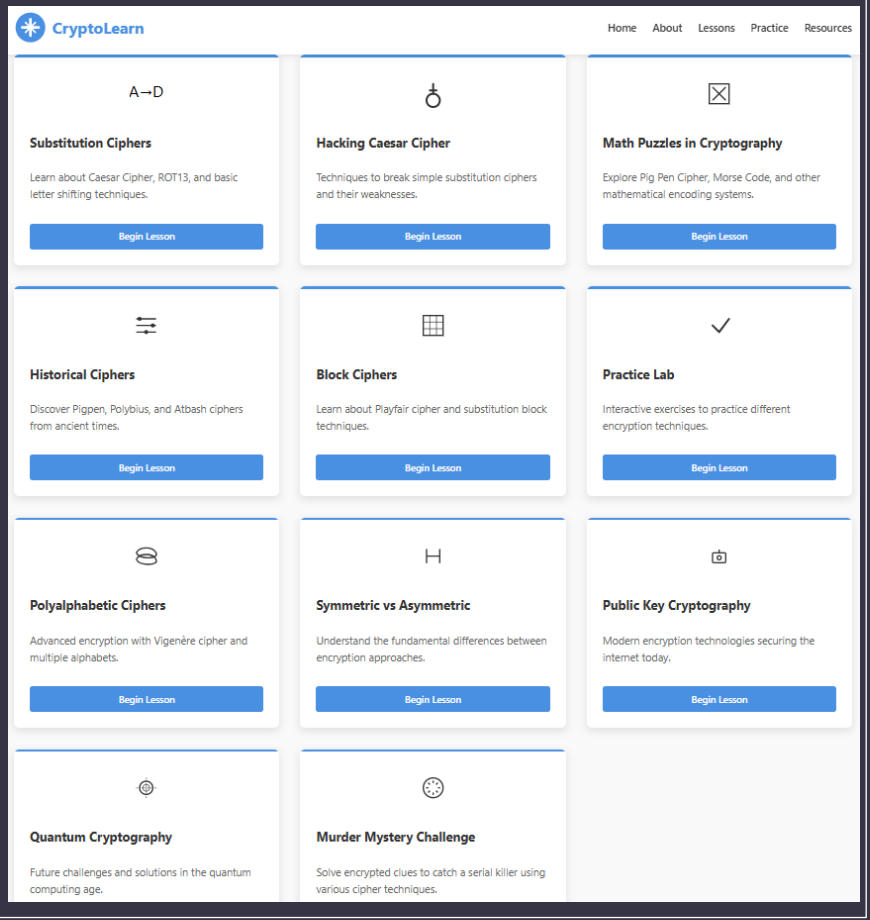
CryptoLearn Platform Overview

CryptoLearn teaches:

- Classical cryptography
- Modern encryption
- Quantum computing fundamentals
- Post-quantum cryptography

Features:

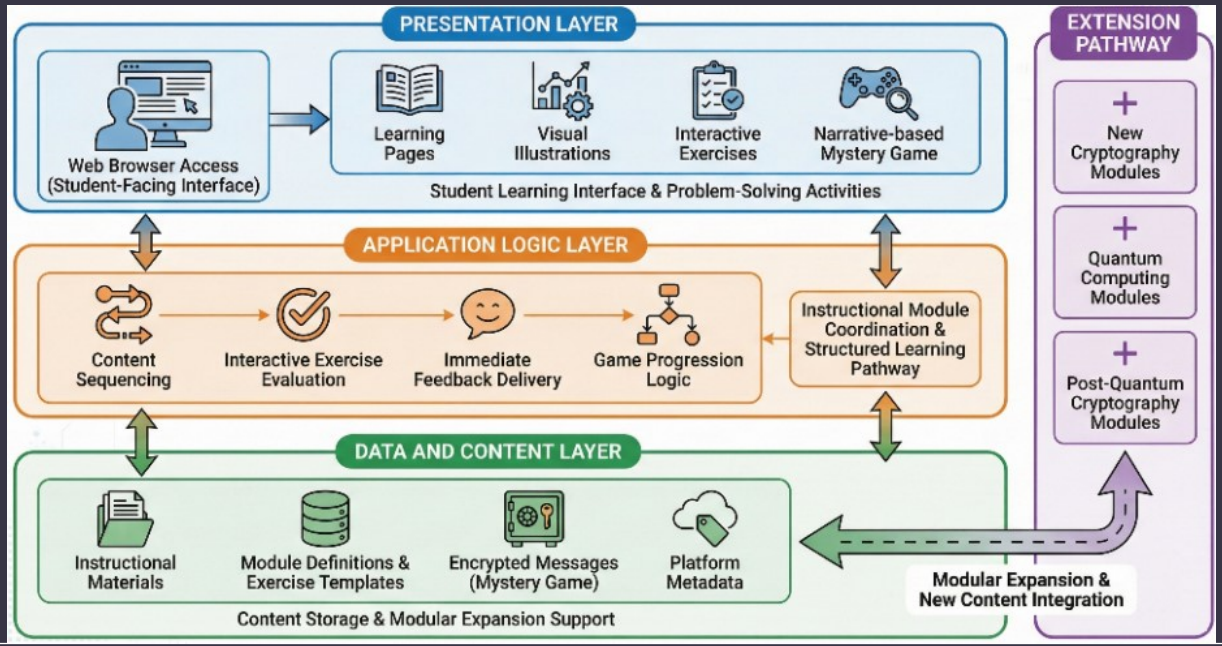
- Interactive lessons
- Visual explanations
- Hands-on exercises
- Narrative-based mystery game



System Architecture

Three-tier architecture:

- Presentation Layer – interface and visualization
- Application Logic Layer – exercises, game logic, navigation
- Data/Content Layer – lessons, exercises, encrypted messages



Learning Module Design

Each module includes:

1. Concept explanation
2. Visual illustration
3. Interactive activity
4. Immediate feedback

Progression:

Basic ciphers → RSA → Quantum computing → Post-quantum cryptography

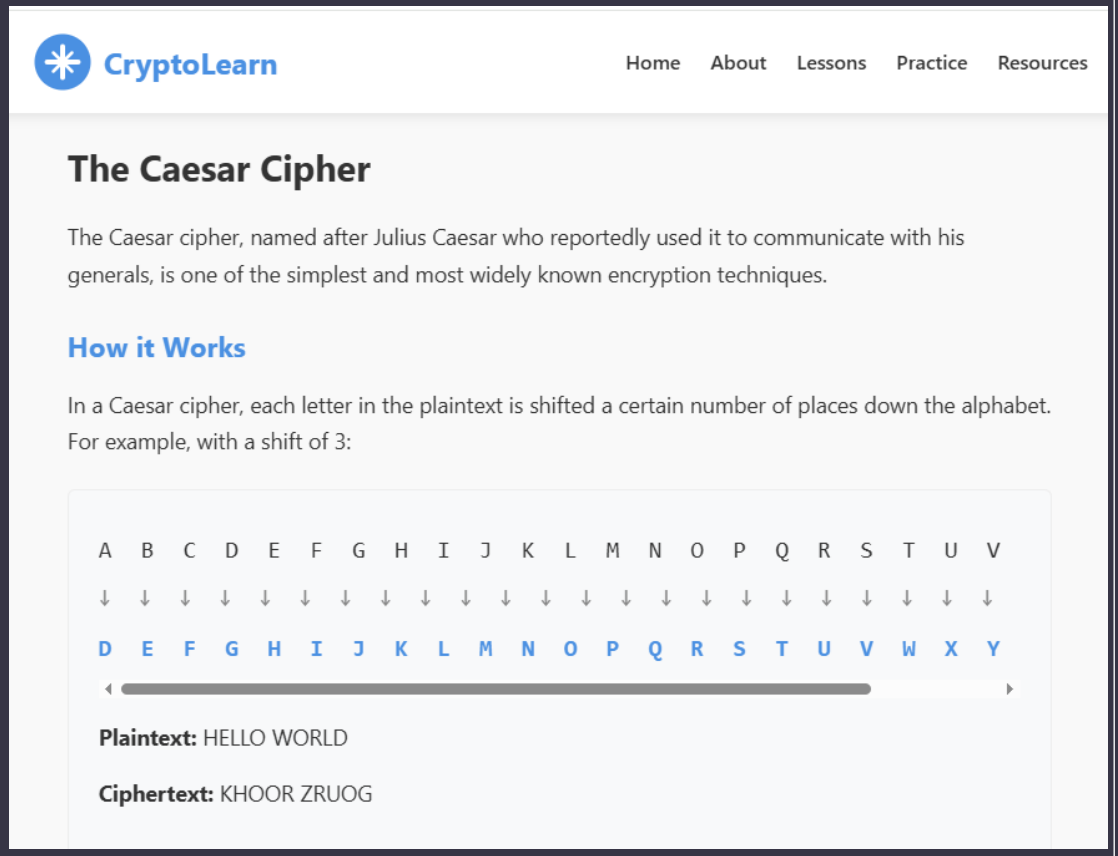
Classical Cryptography Module

Topics:

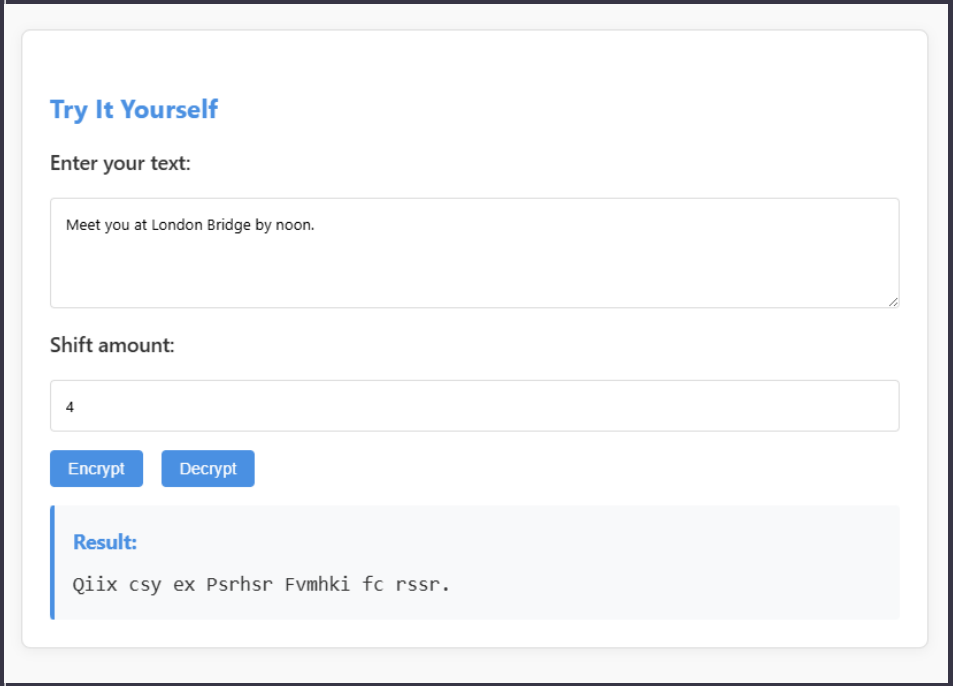
- Caesar Cipher
- Substitution ciphers
- Frequency analysis

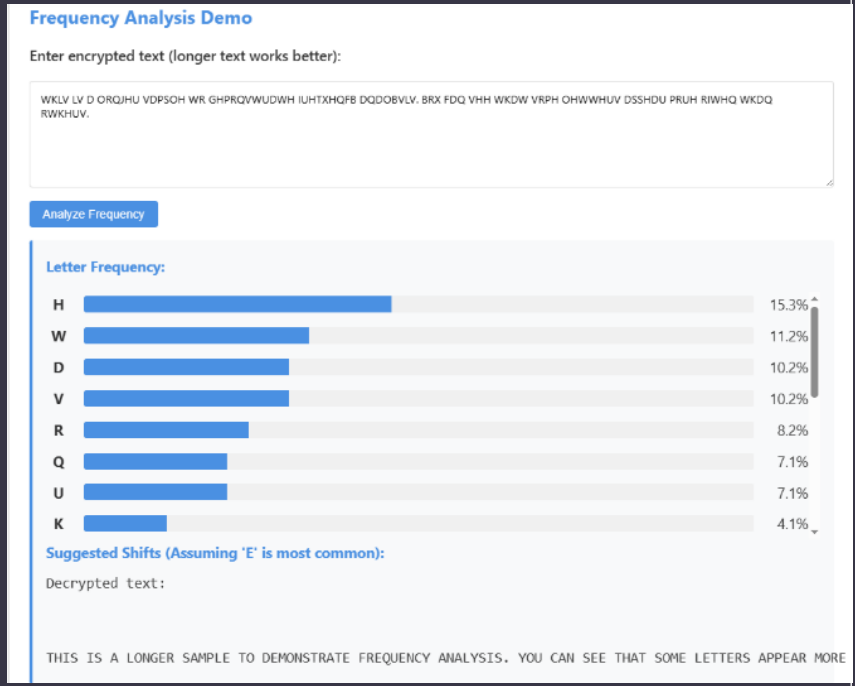
Activities:

- Encryption tools
- Visual alphabet shifting
- Cryptanalysis exercises

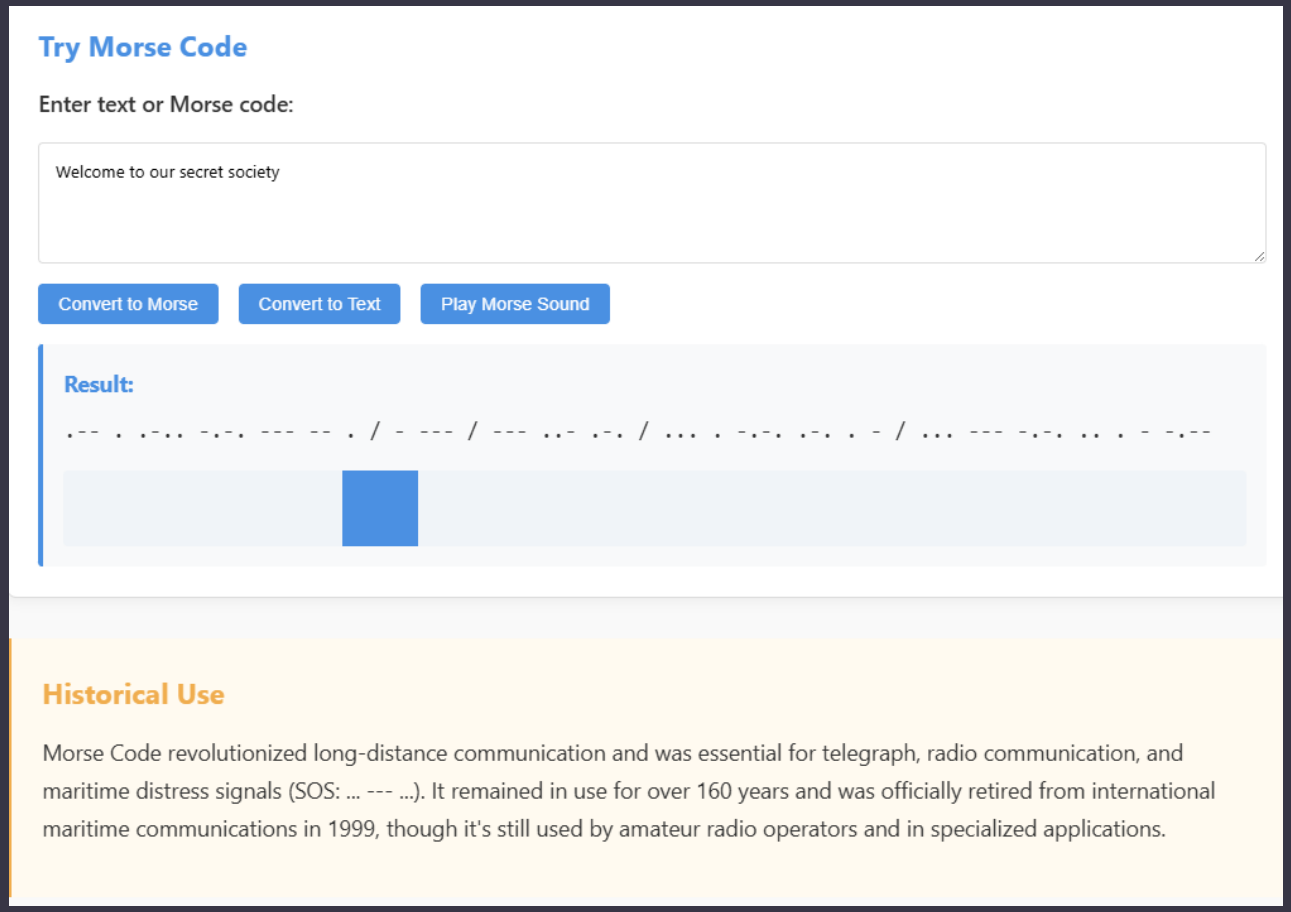


Classical Cryptography Module





Classical Cryptography Module



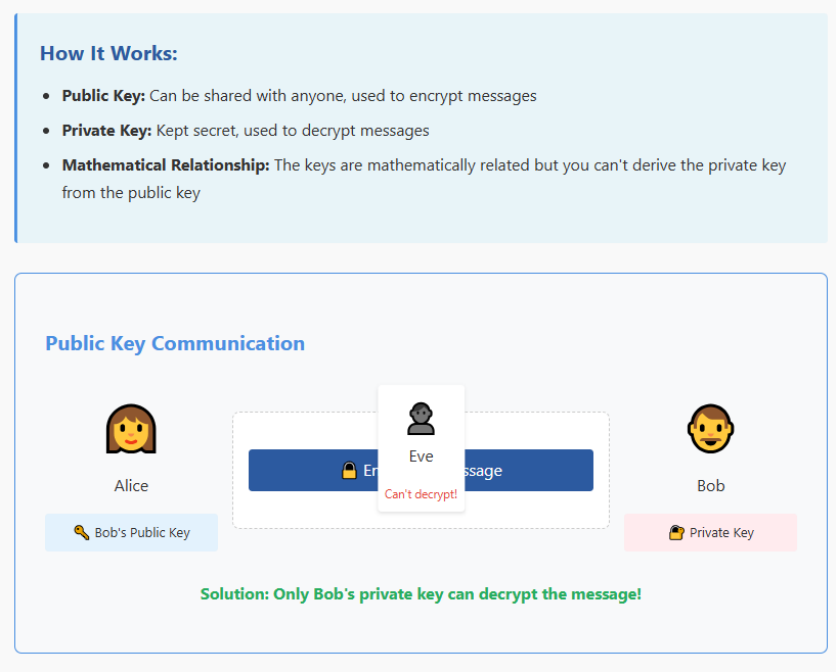
Modern Cryptography Module

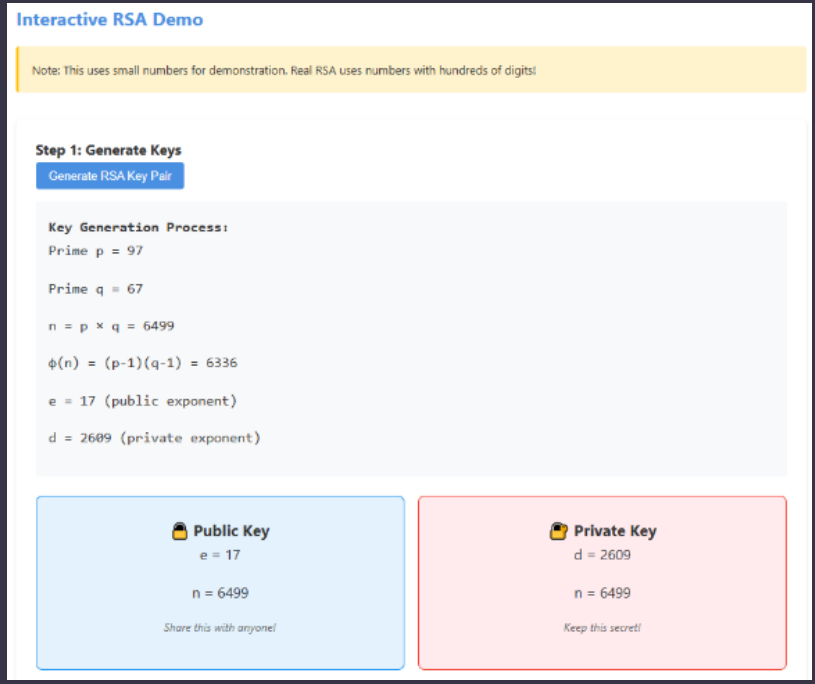
Topics:

- Public-key cryptography
- RSA encryption
- One-way functions
- Encryption vs hashing

Modern Cryptography Module

Interactive RSA demonstrations





Modern Cryptography Module

Test Your Understanding: Quantum Cryptography Transition Quiz

1. Which of the following algorithms is vulnerable to Shor's algorithm?

- ○ A. AES-256
- ◉ B. RSA-2048
- ○ C. CRYSTALS-Kyber
- ○ D. SPHINCS+

2. What is the main principle that makes Quantum Key Distribution secure?

- ○ A. Extremely large key sizes
- ○ B. Complex mathematical problems
- ◉ C. The no-cloning theorem
- ○ D. Multivariate polynomials

3. Which approach is recommended for transitioning to quantum-safe cryptography?

- ○ A. Immediately replace all classical algorithms
- ○ B. Wait until quantum computers are widely available
- ◉ C. Use hybrid schemes combining classical and post-quantum algorithms
- ○ D. Focus exclusively on quantum key distribution

Check Answers

Perfect score: 3/3! You have an excellent understanding of quantum cryptography concepts.

Question 1: RSA-2048 is vulnerable to Shor's algorithm because it relies on the hardness of factoring large numbers, which Shor's algorithm can solve efficiently on a quantum computer.

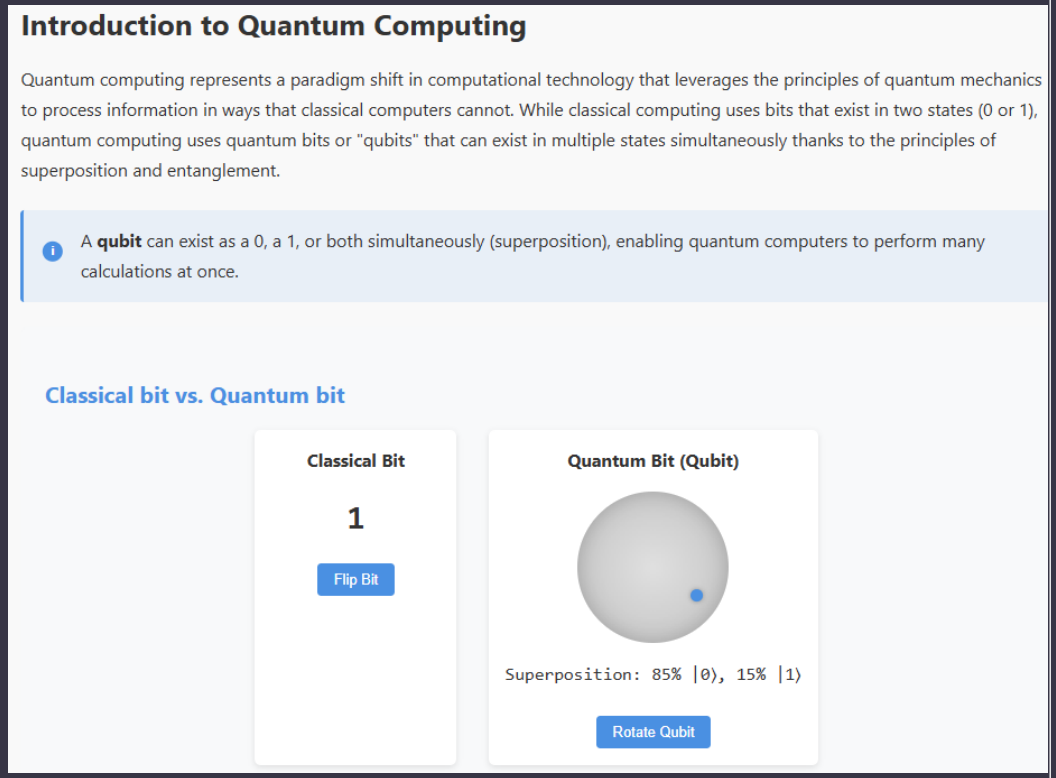
Question 2: Quantum Key Distribution is secure because of the no-cloning theorem, which states that it's impossible to create an identical copy of an unknown quantum state. Any eavesdropping attempt would disturb the quantum state and be detectable.

Question 3: Using hybrid schemes that combine classical and post-quantum algorithms provides the best security during the transition period, ensuring protection even if one algorithm is compromised.

Quantum Computing Module

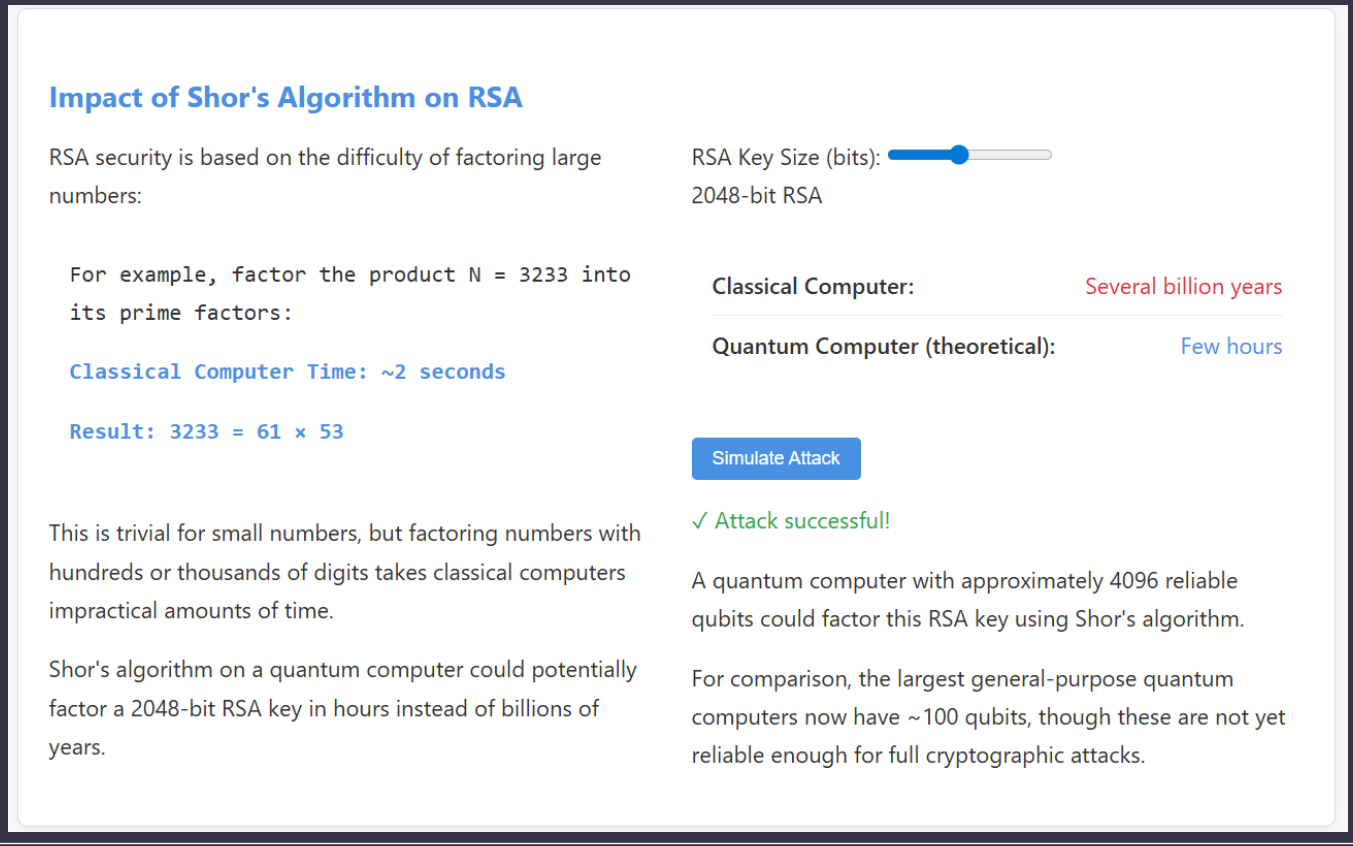
Topics:

- Classical bits vs qubits
- Superposition
- Quantum algorithms
- Shor's algorithm and RSA vulnerability



Quantum Computing Module

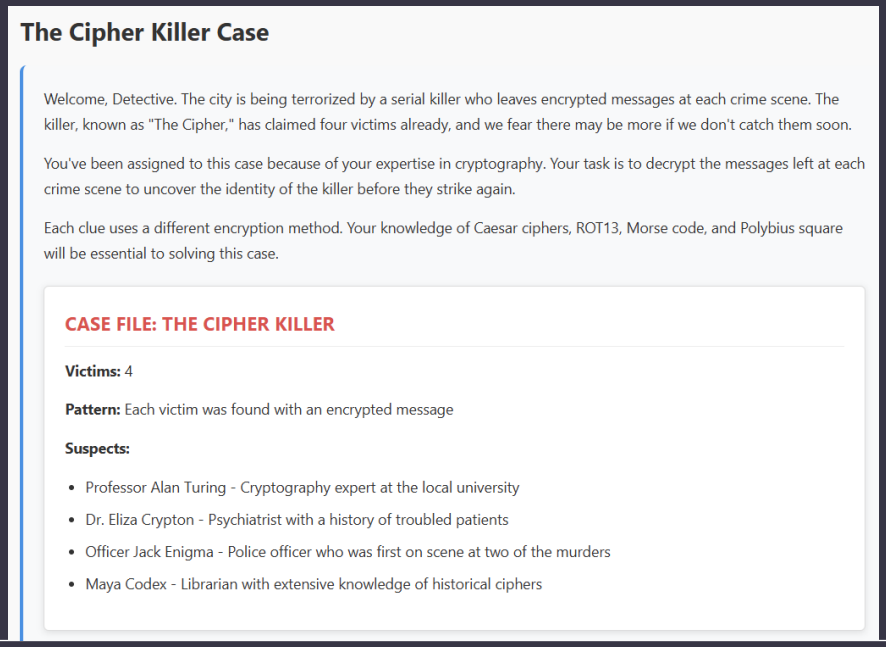
Students use the CryptoLearn simulator to see how algorithms like Shor's algorithm can factor large numbers more efficiently.

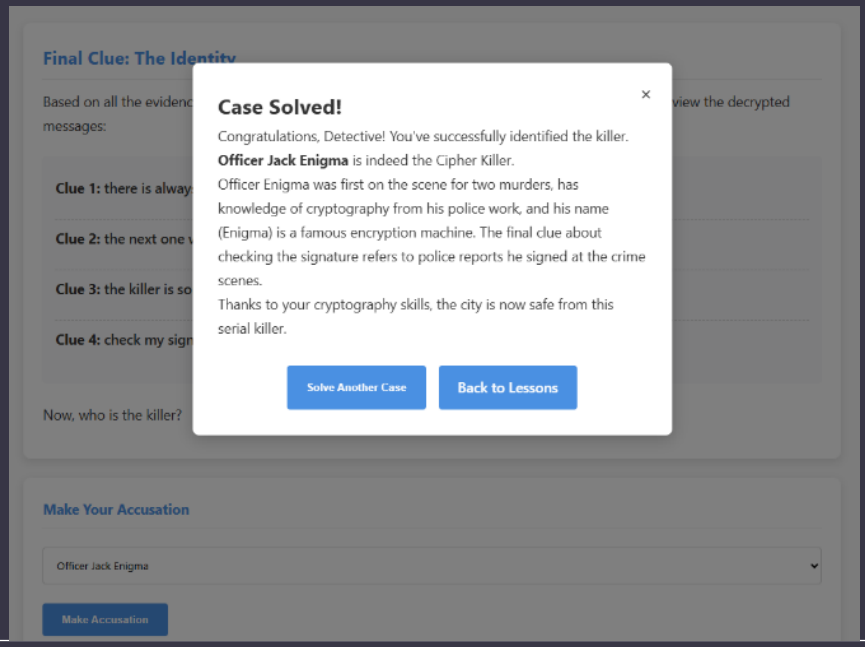


Gamification: The Cipher Killer Case

Students solve a fictional mystery by:

- Decoding encrypted messages
- Applying cryptographic techniques
- Identifying suspects





Deployment and Outreach

Used in:

- CyberSmart workshops (middle school)
- GenCyber camps (high school)
- Community outreach events

Observed Results

- High student engagement
- Positive student perceptions
- Increased curiosity about cybersecurity
- Students can explore independently
- Suitable for high and middle school students
- Students focus on the core concepts and no longer struggle with coding like before
- High retention rate among students

Conclusion

CryptoLearn demonstrates that:

- Complex cybersecurity topics can be introduced early
- Interactive learning improves engagement
- Gamification supports deeper exploration

Future Work

- Conduct structured learning studies
- Implement surveys and assessments
- Expand learning modules
- Add analytics and teacher dashboards

Acknowledgment

- Supported by the Commonwealth Cyber Initiative (CCI)

THANK YOU

Questions, please

abdelhamidse@vmi.edu