

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

Sherif Abdelhamid, James Bangura,
James Jeffers, Mona Aly



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

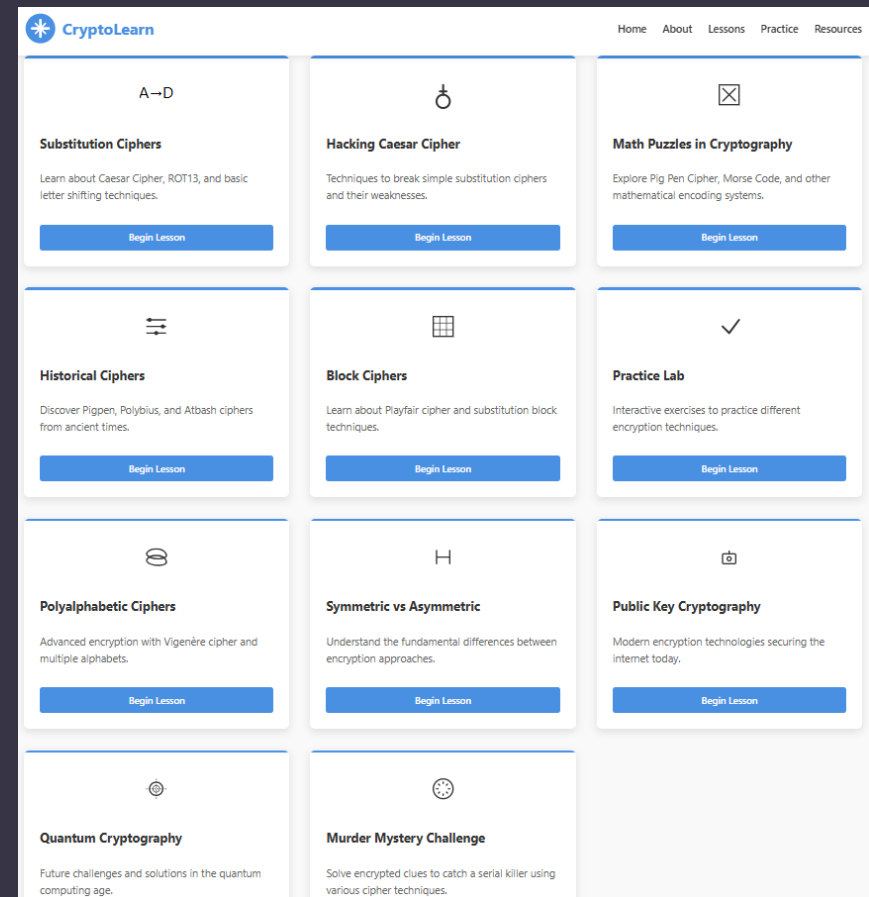
CryptoLearn Platform Overview

CryptoLearn teaches:

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

Features:

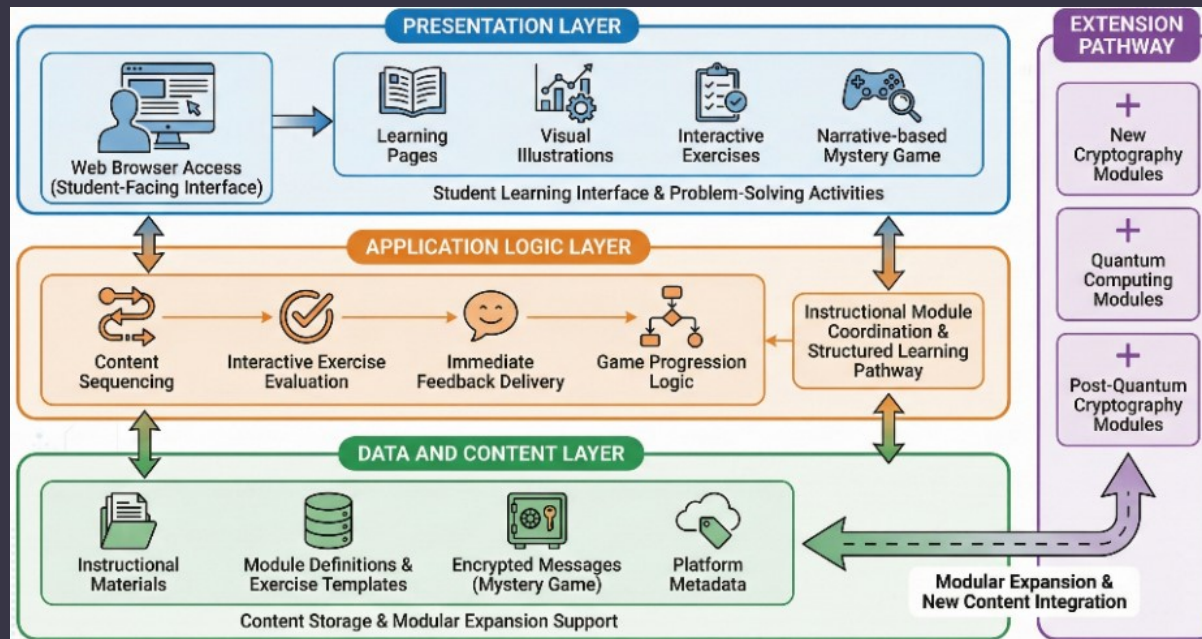
- Interactive lessons
- Visual explanations
- Hands-on exercises
- Narrative-based mystery game



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

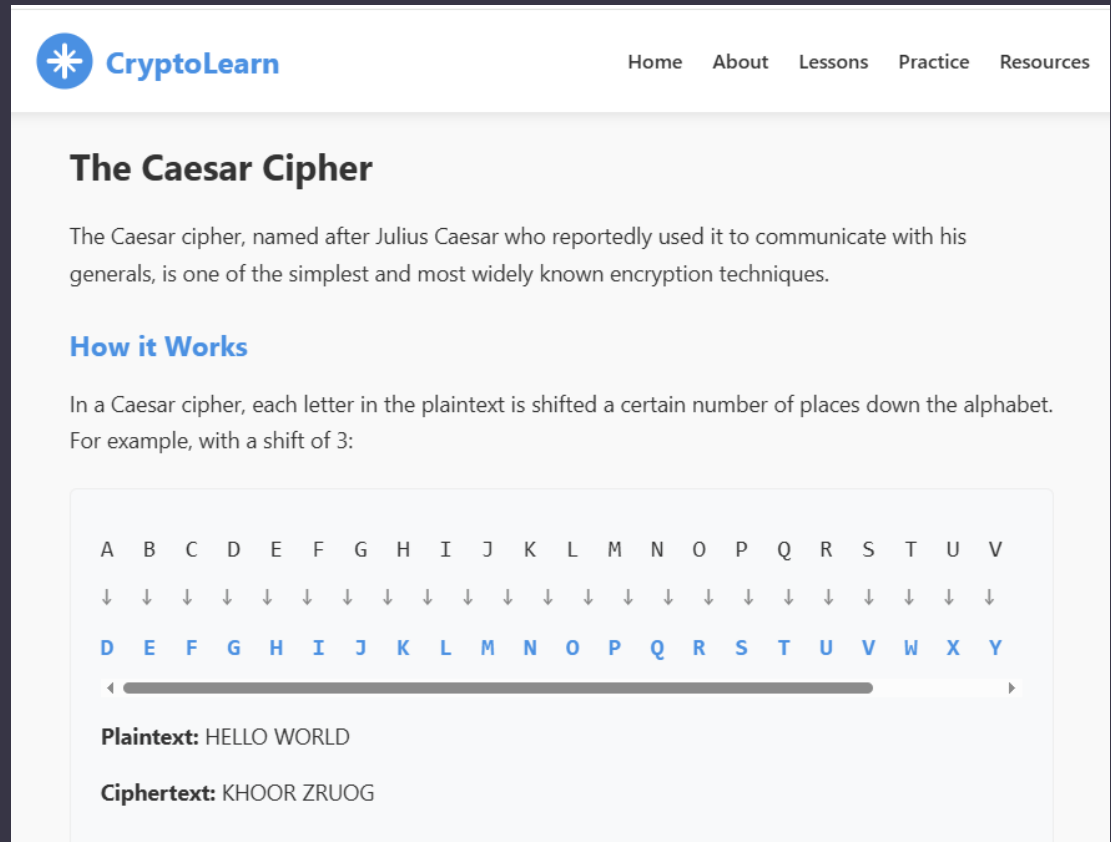
Classical Cryptography Module

Topics:

- Caesar Cipher
- Substitution ciphers
- Frequency analysis

Activities:

- Encryption tools
- Visual alphabet shifting
- Cryptanalysis exercises



The screenshot shows the CryptoLearn website interface. At the top, there is a navigation bar with the CryptoLearn logo (a blue star in a circle) and the text 'CryptoLearn'. To the right of the logo are links for 'Home', 'About', 'Lessons', 'Practice', and 'Resources'. The main content area has a title 'The Caesar Cipher' in bold black text. Below the title is a paragraph: 'The Caesar cipher, named after Julius Caesar who reportedly used it to communicate with his generals, is one of the simplest and most widely known encryption techniques.' Underneath this is a sub-section titled 'How it Works' in blue text. The text below reads: 'In a Caesar cipher, each letter in the plaintext is shifted a certain number of places down the alphabet. For example, with a shift of 3:'. Below this text is a visual diagram of the alphabet shift. It shows two rows of letters: the top row is 'A B C D E F G H I J K L M N O P Q R S T U V' and the bottom row is 'D E F G H I J K L M N O P Q R S T U V W X Y'. Small downward-pointing arrows are positioned between the two rows, indicating the shift. Below the diagram is a horizontal slider with a play button icon on the left and a right-pointing arrow on the right. At the bottom of the diagram area, it shows 'Plaintext: HELLO WORLD' and 'Ciphertext: KHOOR ZRUOG'.

Classical Cryptography Module

Try It Yourself

Enter your text:

Meet you at London Bridge by noon.

Shift amount:

4

Encrypt

Decrypt

Result:

Qiix csy ex Psrhsr Fvmhki fc rssr.

Frequency Analysis Demo

Enter encrypted text (longer text works better):

WKLV LV D ORQJHU VDP SOH WR GHPRQVWUDWH IUHTXHQFB DQDOBLV. BRX FDQ YHH WKDW YRPH OHVWHUHV DSSHU PRUH RIWHQ WKDQ RWKHUV.

Analyze Frequency

Letter Frequency:



Suggested Shifts (Assuming 'E' is most common):

Decrypted text:

THIS IS A LONGER SAMPLE TO DEMONSTRATE FREQUENCY ANALYSIS. YOU CAN SEE THAT SOME LETTERS APPEAR MORE

Classical Cryptography Module

Try Morse Code

Enter text or Morse code:

Welcome to our secret society

Convert to Morse

Convert to Text

Play Morse Sound

Result:

. - - - . - - - . - - - . / - - - / - - - . . . / / . . . - - - . . . - - -

Historical Use

Morse Code revolutionized long-distance communication and was essential for telegraph, radio communication, and maritime distress signals (SOS: ... --- ...). It remained in use for over 160 years and was officially retired from international maritime communications in 1999, though it's still used by amateur radio operators and in specialized applications.

Modern Cryptography Module

Topics:

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

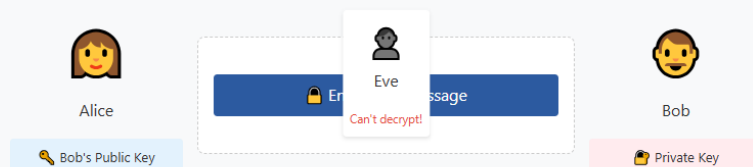
Modern Cryptography Module

Interactive RSA demonstrations

How It Works:

- **Public Key:** Can be shared with anyone, used to encrypt messages
- **Private Key:** Kept secret, used to decrypt messages
- **Mathematical Relationship:** The keys are mathematically related but you can't derive the private key from the public key

Public Key Communication



Solution: Only Bob's private key can decrypt the message!

Interactive RSA Demo

Note: This uses small numbers for demonstration. Real RSA uses numbers with hundreds of digits!

Step 1: Generate Keys

Generate RSA Key Pair

Key Generation Process:

Prime $p = 97$

Prime $q = 67$

$n = p \times q = 6499$

$\phi(n) = (p-1)(q-1) = 6336$

$e = 17$ (public exponent)

$d = 2609$ (private exponent)

Public Key

$e = 17$

$n = 6499$

Share this with anyone!

Private Key

$d = 2609$

$n = 6499$

Keep this secret!

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

Introduction to Quantum Computing

Quantum computing represents a paradigm shift in computational technology that leverages the principles of quantum mechanics to process information in ways that classical computers cannot. While classical computing uses bits that exist in two states (0 or 1), quantum computing uses quantum bits or "qubits" that can exist in multiple states simultaneously thanks to the principles of superposition and entanglement.

- 1 A **qubit** can exist as a 0, a 1, or both simultaneously (superposition), enabling quantum computers to perform many calculations at once.

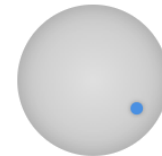
Classical bit vs. Quantum bit

Classical Bit

1

Flip Bit

Quantum Bit (Qubit)



Superposition: 85% $|0\rangle$, 15% $|1\rangle$

Rotate Qubit

Quantum Computing Module

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

Impact of Shor's Algorithm on RSA

RSA security is based on the difficulty of factoring large numbers:

For example, factor the product $N = 3233$ into its prime factors:

Classical Computer Time: ~2 seconds

Result: $3233 = 61 \times 53$

This is trivial for small numbers, but factoring numbers with hundreds or thousands of digits takes classical computers impractical amounts of time.

Shor's algorithm on a quantum computer could potentially factor a 2048-bit RSA key in hours instead of billions of years.

RSA Key Size (bits): 
2048-bit RSA

Classical Computer: **Several billion years**

Quantum Computer (theoretical): **Few hours**

Simulate Attack

✓ **Attack successful!**

A quantum computer with approximately 4096 reliable qubits could factor this RSA key using Shor's algorithm.

For comparison, the largest general-purpose quantum computers now have ~100 qubits, though these are not yet reliable enough for full cryptographic attacks.

Gamification: The Cipher Killer Case

Students solve a fictional mystery by:

- Decoding encrypted messages
- Applying cryptographic techniques
- Identifying suspects

The Cipher Killer Case

Welcome, Detective. The city is being terrorized by a serial killer who leaves encrypted messages at each crime scene. The killer, known as "The Cipher," has claimed four victims already, and we fear there may be more if we don't catch them soon.

You've been assigned to this case because of your expertise in cryptography. Your task is to decrypt the messages left at each crime scene to uncover the identity of the killer before they strike again.

Each clue uses a different encryption method. Your knowledge of Caesar ciphers, ROT13, Morse code, and Polybius square will be essential to solving this case.

CASE FILE: THE CIPHER KILLER

Victims: 4

Pattern: Each victim was found with an encrypted message

Suspects:

- Professor Alan Turing - Cryptography expert at the local university
- Dr. Eliza Crypton - Psychiatrist with a history of troubled patients
- Officer Jack Enigma - Police officer who was first on scene at two of the murders
- Maya Codex - Librarian with extensive knowledge of historical ciphers

Final Clue: The Identity

Based on all the evidence and decrypted messages:

Clue 1: there is always

Clue 2: the next one is

Clue 3: the killer is so

Clue 4: check my sign

Now, who is the killer?

Make Your Accusation

Officer Jack Enigma

Make Accusation

Case Solved!

Congratulations, Detective! You've successfully identified the killer.

Officer Jack Enigma is indeed the Cipher Killer.

Officer Enigma was first on the scene for two murders, has knowledge of cryptography from his police work, and his name (Enigma) is a famous encryption machine. The final clue about checking the signature refers to police reports he signed at the crime scenes.

Thanks to your cryptography skills, the city is now safe from this serial killer.

Solve Another Case

Back to Lessons

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