Interactive Classical Ciphers for Cybersecurity Education

SNEHA & YASHASHRI | 10TH MAY 2025

Agenda

- 1. Introduction & Problem
  - 2. Solution & Objectives
  - 3. Architecture & Tech Stack
  - 4. Implementation Details
  - 5. Cipher Deep Dives
  - 6. Evaluation & Results
  - 7. Use Cases & Benefits
  - 8. Future Scope & References

Introduction

- • Cryptography as cornerstone of cybersecurity
  - Secures confidentiality, integrity, authenticity
  - Critical against threats: eavesdropping, tampering, replay
  - Foundational for protocols: TLS, VPN, secure messaging

Problem Statement

- • Traditional teaching is theory-heavy
  - Abstract math concepts hard to visualize
  - Limited hands-on practice with real ciphers
  - Low engagement and retention rates

Solution & Objectives

- • Web-based interactive platform
  - Implement Caesar, Playfair, Hill, Affine ciphers
  - Enable real-time key generation & visualization
  - Enhance engagement through interactive UI
  - Evaluate learning gains and usability

Architecture & Tech Stack

- • Client-side application
  - HTML5 & CSS3 (Grid, Flexbox) for responsive design
  - Vanilla JavaScript for cipher logic
  - No server dependencies — preserves privacy
  - Modular codebase for easy extension

Implementation Overview

- • Card-based homepage for cipher selection
  - Interactive matrix display for Playfair
  - Animated transitions for clarity
  - Responsive layout for mobile & desktop
  - Clean and neat design

Caesar Cipher Deep Dive

- • Shift-based substitution cipher
  - letterToNumber() & numberToLetter() helpers
  - Encryption: (x + shift) % 26
  - Decryption: (x - shift + 26) % 26
  - Use case: Demonstrates basic substitution

Playfair Cipher Deep Dive

- • Bigram substitution using 5x5 matrix
  - generateKeyMatrix(keyword) function
  - prepareText(): handles J→I, duplicate letters, padding
  - Encrypt/decrypt rules for rows, columns, rectangles
  - Visualization of matrix and letter pair movements

Hill Cipher Deep Dive

- • Matrix-based polygraphic cipher
  - 2x2 key matrix input & determinant coprimality check
  - encrypt: multiply plaintext vector by key matrix mod 26
  - decrypt: compute inverseMatrix() via adjugate & mod inverse
  - Illustrates linear algebra in cryptography

Affine Cipher Deep Dive

- • Linear function cipher
  - Encryption: $E(x) = (a*x + b) \bmod 26$
  - Decryption: $D(y) = a^{-1} * (y - b) \bmod 26$
  - Valid 'a' values must be coprime with 26
  - Demonstrates modular arithmetic concepts

Evaluation & Results

- • Mixed-methods study with 30 students
  - 35% average improvement in pre/post tests
  - SUS score of 82 (above 68 benchmark)
  - Positive qualitative feedback on engagement
  - Observed deeper conceptual understanding

Real-World Use Cases

- • Educational Environments
  - University and secondary school curricula
  - Corporate cybersecurity training programs
  - MOOCs and self-paced online courses
  - Capture The Flag (CTF) competition warm-ups

Benefits to Cybersecurity

- • Strengthens core cryptographic skills
  - Prepares learners for modern encryption algorithms
  - Encourages secure implementation practices
  - Improves problem-solving and analytical skills
  - Builds confidence in handling real-world security tasks

Future Scope & References

- • Future Enhancements
  - Integrate RSA, AES modules with visual steps
  - Add gamified quizzes and achievement badges
  - Develop instructor dashboards & progress tracking
  - Convert to PWA for offline/mobile use
  - References available in full paper