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

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

Sherif Abdelhamid[1], James Bangura[2], James Jeffers[3], Mona Aly[4]

[1]Virginia Military Institute
[2]Virginia Military Institute, USA
[3]Virginia Military Institute, USA
[4]Independent Researcher, USA

Abstract

Introducing students to advanced topics such as cryptography, quantum computing, and post-quantum cryptography at an early age is essential for preparing the next generation to navigate a rapidly evolving digital landscape. This paper presents CryptoLearn, a web-based educational platform designed to make these complex subjects accessible to middle school, high school, and undergraduate students. The platform employs simple, easy-to-understand language, illustrations, and interactive exercises that provide immediate feedback. To further enhance engagement, CryptoLearn integrates game-based learning, including a mystery game in which students decipher encrypted messages to solve a storyline-based challenge. The platform was implemented using a multi-tier architecture that ensures extensibility, allowing new modules and topics to be seamlessly added over time. To date, CryptoLearn has been deployed in multiple educational contexts, including the CyberSmart workshop for middle school students, the GenCyber camp for high school students, and broader outreach initiatives. Preliminary feedback from participants indicates highly positive perceptions and observable increases in student engagement and motivation. These findings suggest that the combination of interactive exercises, gamification, and narrative-driven activities can serve as effective approaches for introducing advanced computing topics to younger learners. Future work includes conducting structured student-focused studies, including surveys and interviews, to systematically measure the platform's impact on learning outcomes, motivation, and long-term interest in cryptography and related fields. Using advanced computing topics with accessible pedagogy and engaging digital formats, CryptoLearn represents an innovative pathway for equipping students with the foundational knowledge and critical thinking skills necessary for the cybersecurity challenges of tomorrow.

Keywords: *Cryptography education, Quantum computing, Post-quantum cryptography, Game-based learning, Student engagement, Interactive learning, STEM outreach*

1. Introduction

1.1 Background

Cybersecurity and cryptography are increasingly essential components of modern digital literacy. As society becomes more dependent on secure communication, encrypted data storage, and emerging technologies such as quantum computing, there is a growing recognition that students must develop foundational knowledge of these topics much earlier than in traditional curricula. However, cryptography and quantum concepts are typically introduced only at advanced secondary or undergraduate levels, where learners may encounter steep conceptual barriers due to abstract mathematical foundations and a lack of prior exposure. Recent educational research emphasizes the importance of early intervention, interactive learning tools, and scaffolded instruction to build long-term engagement in STEM fields. This creates an opportunity to design learning environments that translate complex topics into accessible, age-appropriate formats.

1.2 Motivation

Despite the expanding global demand for cybersecurity skills, few platforms are specifically designed to introduce cryptography, post-quantum cryptography, and quantum computing to middle school and high school learners. Existing resources often rely on static text, lack interactivity, or assume prior technical knowledge. These limitations reduce accessibility and may discourage learners who would

otherwise benefit from early exposure to cybersecurity concepts. Motivated by the need for inclusive, engaging, and pedagogically grounded tools, the CryptoLearn platform was designed to simplify difficult concepts through intuitive explanations, illustrations, interactive exercises, and narrative-driven game mechanics. A key objective is not only to convey core ideas but also to enhance students' motivation and curiosity by embedding content within a meaningful, problem-solving–oriented storyline. Deployments in educational workshops have shown promising signs of increased engagement and interest among learners, reinforcing the need for scalable digital platforms that support early STEM and cybersecurity education.

1.3 Overview of the CryptoLearn Platform

CryptoLearn is a web-based learning platform built using a multi-tier architecture that supports modular expansion. The platform introduces students to classical cryptography, modern encryption techniques, quantum computing fundamentals, and post-quantum cryptography through simplified language and rich visual explanations. Interactive exercises provide immediate feedback, enabling students to apply concepts in real time. The platform also includes a narrative-based mystery game in which students decode encrypted clues to solve a fictional case, reinforcing learning through gamified exploration. CryptoLearn has been deployed during the CyberSmart workshop (middle school), the GenCyber camp (high school), and multiple outreach activities, with participants expressing positive perceptions and strong levels of engagement.

1.4 Contributions

This paper makes the following contributions:

1. Design and Development of CryptoLearn: We present a scalable, web-based learning platform that introduces cryptography, quantum computing, and post-quantum cryptography to younger learners using accessible language, illustrations, and interactive modules.
2. Integration of Game-Based Learning: The platform incorporates gamified activities and a mystery game that embeds cryptographic challenges within a narrative-driven storyline to enhance engagement and promote active learning.
3. Empirical Deployment and Observations: We report on the platform's use in real educational contexts—CyberSmart, GenCyber, and outreach events—and describe preliminary findings on student engagement and perceptions.
4. Extensible Multi-Tier Architecture: We describe the system architecture that allows easy expansion through new modules, exercises, and learning activities as cryptographic and quantum technologies evolve.

2. Related work

Cryptography has long been recognized as a powerful interdisciplinary tool for teaching mathematical reasoning, computational thinking, and problem-solving skills. Early work by Sakalli and Bulus demonstrated that cryptography can enrich mathematics education by illustrating abstract concepts such as modular arithmetic, functions, and number theory through concrete encryption algorithms and cryptanalysis exercises [1]. Their study highlighted the value of ciphers, puzzles, and games in increasing high school students' enthusiasm for mathematics, computer science, and electronics, establishing a pedagogical foundation for later game-based and activity-driven cryptography instruction.

More recent efforts have expanded cryptography education into secondary and undergraduate contexts using interactive and visual learning materials. Yamaguchi et al. developed graphical teaching materials and online applications to introduce cryptography concepts to senior high school students, emphasizing simplified explanations of the mathematical foundations of security to address gaps in traditional textbooks [2]. Similarly, Rao and Dave proposed hands-on laboratory exercises using emerging technologies such as blockchain and the Internet of Things, demonstrating that cryptographic concepts such as hash functions can be made accessible to undergraduate STEM students through applied, experiential learning [3]. Recent work has also explored the role of visual and collaborative learning environments in improving cryptography education. Abdelhamid et al. investigated the use of collaborative visual programming to enhance students' understanding of cryptographic concepts, demonstrating that visual abstractions and shared problem-solving

environments can reduce cognitive barriers and support conceptual reasoning in cryptography instruction [4].

As quantum computing has emerged as a disruptive threat to classical public-key cryptography, several studies have explored instructional approaches for teaching post-quantum cryptography (PQC). Jamshidi et al. investigated active learning strategies for introducing PQC concepts to undergraduate and graduate students, comparing traditional lectures with student-led seminars and interactive activities such as coding exercises and game-based assessments [5]. Their findings indicate that active and student-centered approaches significantly improve engagement and learning outcomes, particularly at advanced academic levels. Complementing this work, Borrelli et al. described the design and delivery of a dedicated post-quantum cryptography course, covering lattice-based, code-based, and hash-based schemes, and demonstrated that upper-level undergraduate students can successfully engage with PQC topics when content is carefully scaffolded [6].

Other researchers have explored modular and incremental approaches to PQC education. Borrelli et al. proposed a modular curriculum framework that distinguishes between awareness-level and proficiency-level instruction, enabling PQC concepts to be introduced across high school, undergraduate, and graduate contexts with appropriate depth [7]. Pérez-Ramos et al. introduced GeoGebra-based activities to teach lattice concepts relevant to PQC at the high school level, leveraging familiar mathematical tools to lower the entry barrier to an otherwise abstract topic [8]. In parallel, Holden provided a comprehensive resource guide for teaching post-quantum cryptography, outlining systems suitable for introductory courses and highlighting simplified variants that can be adapted for undergraduate instruction [9]. Holden also introduced Alkaline, a reduced-complexity variant of the Kyber algorithm, designed specifically for classroom use to illustrate post-quantum encryption principles without overwhelming students [10].

More recently, immersive and multi-modal learning environments have been explored as mechanisms for teaching cryptography and cybersecurity concepts. Abdelhamid et al. presented CryptoQuest, an extended reality (XR)–based interactive animation series targeting high school and university students, integrating gamification, animation, and immersive technologies to teach classical cryptography, quantum computing, and post-quantum cryptography [11]. This work underscores the growing interest in narrative-driven and experiential learning approaches for conveying complex cybersecurity concepts.

3. System Design

The design of CryptoLearn follows a multi-tier architectural model that supports scalability, modularity, and long-term extensibility. The system was intentionally structured to accommodate evolving topics in cryptography and quantum technologies while enabling the addition of new pedagogical features, such as interactive exercises, assessments, and game-based learning modules. This section details the guiding design principles, architectural layers, and pedagogical elements that underpin the platform.

3.1 Design Goals

The development of CryptoLearn was guided by several key objectives:

- Accessibility: Provide clear, intuitive explanations and interactive visualizations suitable for middle school, high school, and early undergraduate learners.
- Pedagogical Effectiveness: Integrate evidence-based instructional strategies such as immediate feedback, scaffolded progression, and narrative-based learning.
- Modularity and Extensibility: Enable seamless expansion of learning modules to incorporate new topics (e.g., additional ciphers, post-quantum algorithms, quantum concepts).
- Usability and Engagement: Design a user-friendly interface supported by gamification elements to motivate sustained exploration.
- Platform Flexibility: Utilize a web-based architecture to ensure compatibility across devices and accessibility without installation requirements.

3.2 Multi-Tier Architecture

CryptoLearn is implemented using a three-tier architecture (see Figure 1) consisting of the presentation layer, application logic layer, and data/content layer. This approach decouples user interaction from backend logic and content management, enabling scalability and maintainability.

The presentation layer constitutes the platform's user interface, rendered in the browser and responsible for delivering instructional content, illustrations, and interactive components. User navigation, animations, and visual feedback mechanisms are handled within this tier. The design prioritizes clarity, simplicity, and responsiveness to accommodate a broad age range and a variety of devices. The application logic layer manages the platform's dynamic behavior, including Interactive exercises that check correctness and provide immediate feedback. Game mechanics such as clue progression and state management within the mystery storyline. Routing and content sequencing that guide students through modules. Logging and tracking of student interactions (where implemented), enabling future integration of analytics or adaptive learning. The data/content layer stores instructional materials, exercise templates, encrypted messages for the game-based module, and metadata related to learning modules. By separating content from logic, the platform can be easily extended with new topics or activities. Instructors or developers can add modules without altering the underlying system design.

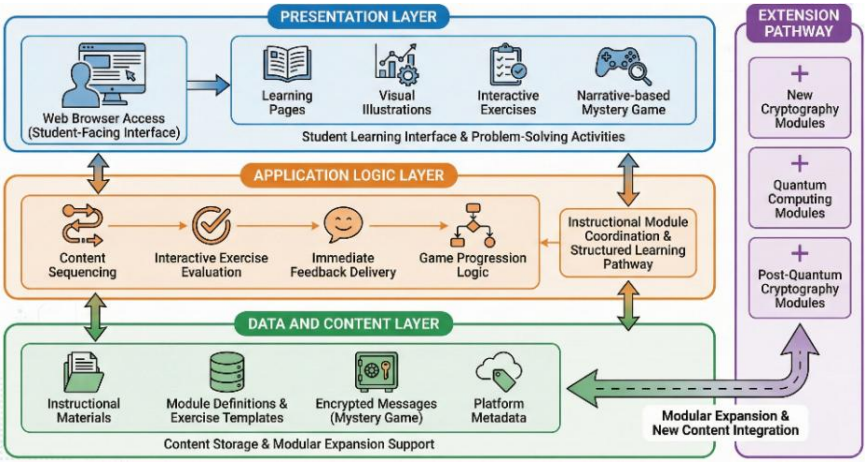

Fig. 1. Multi-tier architecture of the CryptoLearn Platform.

3.3 Learning Module Structure

Each learning module (from classical encryption to quantum and post-quantum topics) is designed around a consistent structure:

- Conceptual Introduction: Simple explanations using accessible language.
- Illustrations and Visual Aids: Graphical representations to clarify abstract ideas such as bit operations, qubits, or encryption transformations.
- Interactive Activities: Students apply concepts through small exercises (e.g., encryption/decryption tasks, drag-and-drop matching, or fill-in-the-blank quizzes).
- Immediate Feedback: Automated evaluation provides corrective guidance, reinforcing conceptual understanding.

Modules progress from foundational ideas (e.g., Caesar cipher) to more advanced concepts (e.g., RSA, quantum states, post-quantum lattice-based schemes), creating a scaffolded learning trajectory.

3.4 Gamification and Narrative-Based Learning

A distinctive feature of CryptoLearn is its narrative-driven mystery game, which motivates students through problem-solving and exploration. In this module, Students play the role of investigators attempting to solve a fictional crime. The "villain" leaves encrypted messages using various ciphers learned throughout the course. Students must decipher the messages to progress through the storyline. This gamification strategy incorporates core engagement principles (challenge, narrative immersion, and immediate feedback). As students decode messages, they reinforce theoretical concepts while engaging with cryptography in a meaningful context.

4. System Implementation

4.1 User Interface and Interaction Design

The interface was intentionally designed to resemble modern educational applications that students are already comfortable using. Key design principles include: 1) visual clarity: use of illustrations,

diagrams, and color cues to explain abstract concepts. 2) progressive disclosure: presenting information gradually to prevent overload, especially when introducing complex mathematical or quantum ideas. 3) immediate feedback mechanisms: when students complete exercises, the platform instantly indicates correctness and provides hints or explanations, reinforcing understanding. 4) low barrier to entry: activities require no prior knowledge of programming or advanced mathematics.

4.2 Structure of the Learning Modules

Each module consists of four recurring components: (1) conceptual explanation, (2) visual illustration, (3) interactive activity, and (4) immediate feedback.

4.2.1 Classical Cryptography Module

This module introduces fundamental encryption concepts through intuitive examples and historical ciphers. Key topics include:

- Caesar Cipher and Shift Operations: Students apply shifts, as shown in Figure 2, to encode and decode messages using drag-and-drop or fill-in-the-blank interactions.

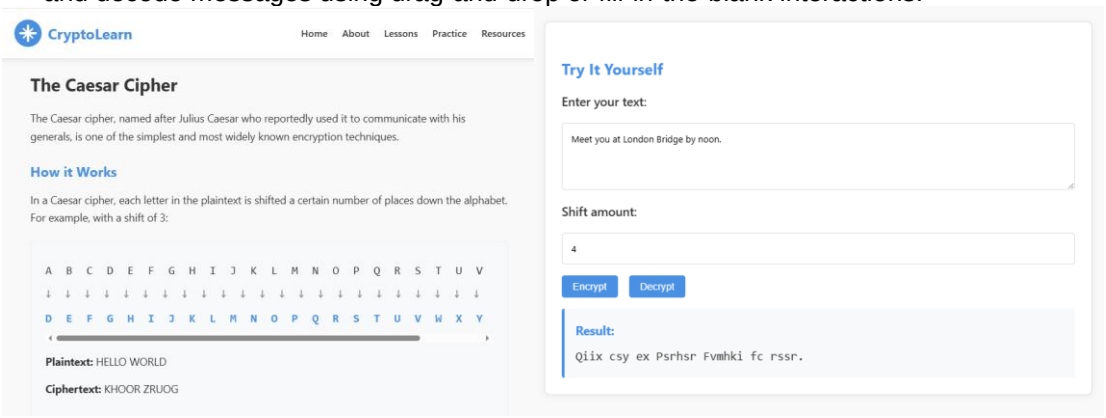

Fig. 2. Interactive Caesar cipher learning module in the CryptoLearn platform, illustrating concept explanation, visual letter shifting, and a hands-on encryption/decryption activity with immediate feedback.

- Substitution Ciphers: Learners explore the idea of mapping letters and patterns, observing how patterns reveal weaknesses in simple schemes.
- Frequency Analysis: Basic exercises show how letter frequencies (see Figure 3) can be used to break simple ciphers, reinforcing critical thinking.

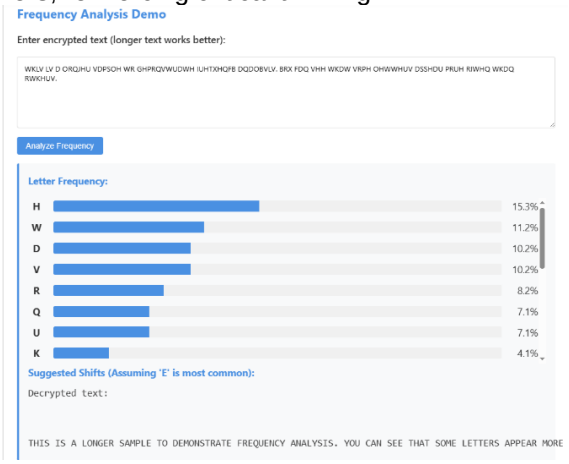

Fig. 3. Frequency analysis demonstration in the CryptoLearn platform, showing letter distribution visualization and suggested shifts to support cryptanalysis of encrypted text.

4.2.2 Modern Cryptography Module

This module introduces concepts that underpin real-world secure communication techniques. Although simplified, these lessons provide early exposure to ideas students will encounter in later coursework. Topics include:

- Public-Key Cryptography Principles: Illustrated explanations (see Figure 4) of how two keys work together to encrypt and decrypt messages.

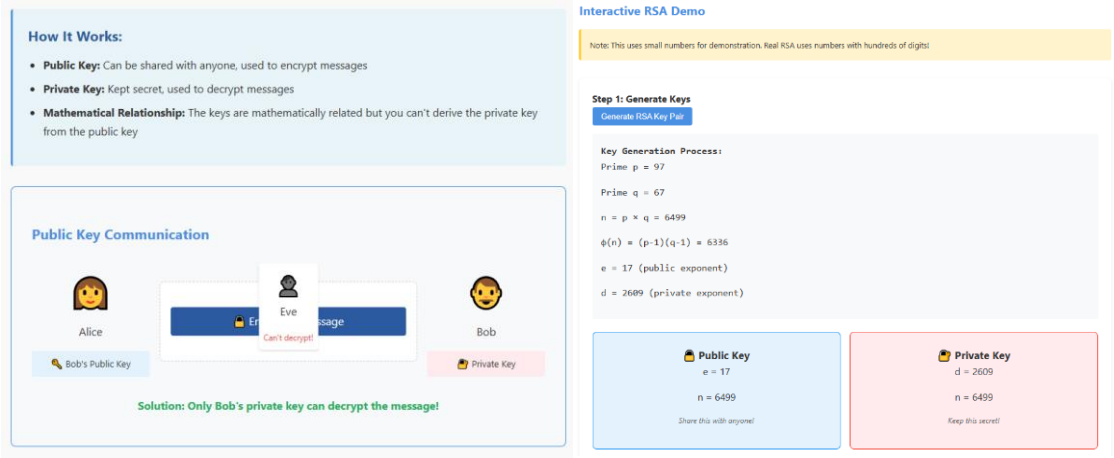

Fig. 4. Public-key cryptography and RSA learning module in the CryptoLearn platform.

- Simplified RSA Concepts: Students experiment with small numerical examples that demonstrate one-way functions without requiring advanced mathematics.
- Encryption vs. Hashing: Clear distinctions between secrecy and integrity are reinforced through interactive comparisons.

4.2.3 Quantum Computing Module

Given the growing importance of quantum technologies, this module introduces foundational ideas such as: 1) Qubits and Superposition: Presented through visual metaphors and animations (see Figure 5) that show simultaneous states, 2) Quantum vs. Classical Computation: Students compare how classical bits and qubits behave differently, and 3) Quantum Algorithms in Context: High-level explanations (e.g., Shor's algorithm) illustrate why quantum computing threatens classical cryptography.

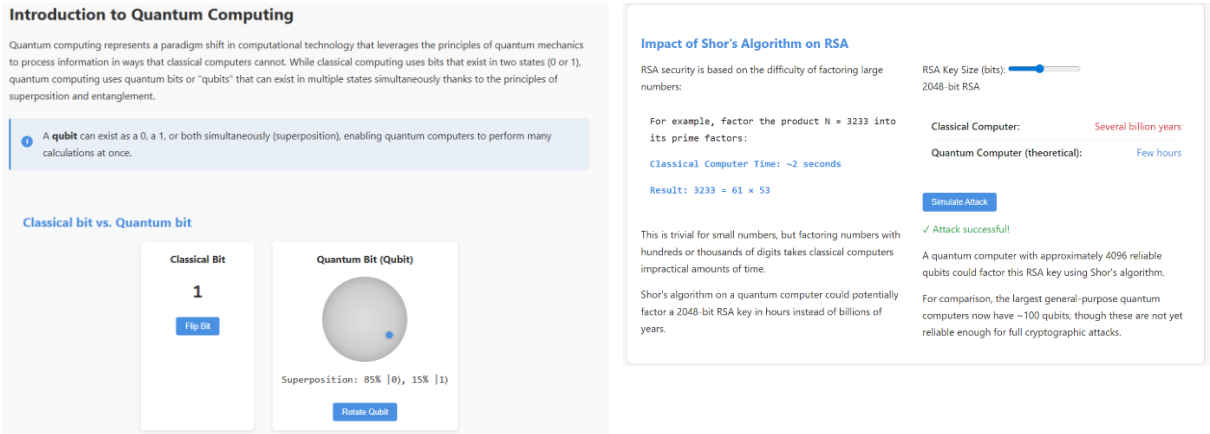

Fig. 5. Quantum computing learning module illustrating fundamental differences between classical bits and qubits, and demonstrating the impact of Shor's algorithm on RSA security through interactive visualizations.

4.2.4 Post-Quantum Cryptography Module

As quantum threats become more relevant, the module introduces the next generation of cryptographic protections:

- Motivation for Post-Quantum Schemes: Illustrated scenarios show how quantum computers could break current systems.
- High-Level Overview of Lattice-Based Cryptography: Simple analogies explain the hardness of the shortest vector problem.
- Transition to Quantum-Resistant Standards: Students learn how new algorithms are designed to withstand quantum threats.

4.2.5 Integration of Interactive and Gamified Components

To reinforce learning, each conceptual topic includes carefully designed interactive elements such as: encryption/decryption simulators, multiple-choice challenges, matching games, drag-and-drop workflows, and puzzle-based exercises. The mystery game (see Figure 6) integrates these activities into a narrative, requiring students to apply their emerging knowledge to decode clues left by a fictional villain. This connection between theory and practice strengthens retention and promotes active problem-solving.

5. Deployment and Outreach

CryptoLearn has been deployed in several educational and community settings to introduce cryptography and quantum-related concepts to diverse groups of learners. These deployments served both instructional and evaluative purposes, allowing the platform to be tested with real students while providing insights into engagement patterns, usability, and overall learner perceptions.

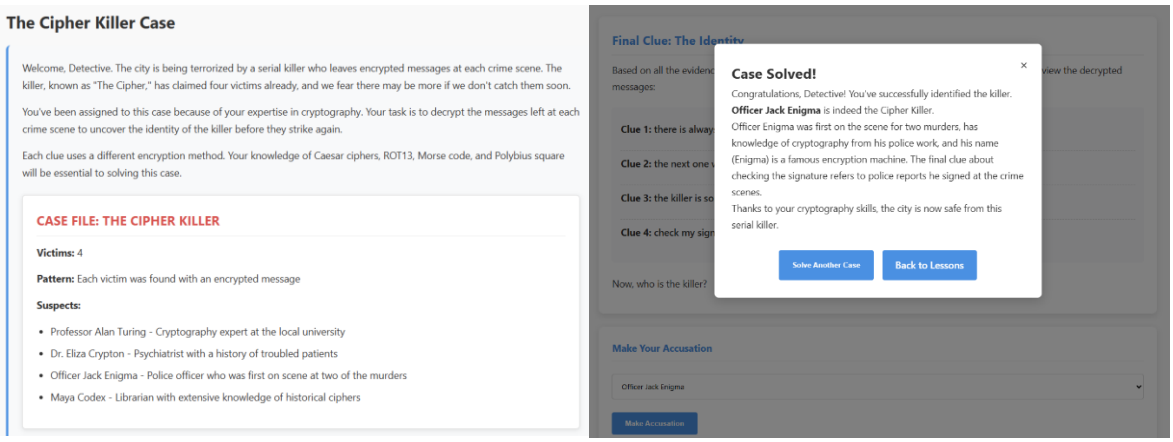

Fig. 6. Narrative-based mystery game in the CryptoLearn platform, where students apply cryptographic techniques to decode clues, identify suspects, and solve a fictional crime through interactive, game-driven learning.

5.1 Deployment in the CyberSmart Workshop (Middle School)

The CyberSmart Workshop is an annual cybersecurity education initiative, sponsored by CyDef Lab at Virginia Military Institute, that introduces middle school students to foundational digital literacy and safety concepts. CryptoLearn was integrated into the workshop as a central instructional tool to teach basic cryptography principles through interactive modules and age-appropriate games. Students navigated classical cipher lessons, completed short encryption exercises, and participated in the mystery storyline by decoding simple encrypted clues. Despite the abstract nature of cryptography, participants demonstrated strong enthusiasm for the interactive components, particularly the puzzle-based activities. The immediacy of feedback and the use of graphical explanations helped reduce cognitive barriers commonly encountered by younger learners encountering cryptography for the first time.

5.2 Deployment in the GenCyber Workshop (High School)

CryptoLearn was also used in the GenCyber high school program, a cybersecurity-focused camp funded by the National Security Agency. High school participants were introduced to both classical and modern cryptographic concepts, including simplified explanations of public-key cryptography and introductory material on quantum computing. The platform's interactive modules allowed students to experiment with encryption and decryption, while the narrative-based mystery game provided a practical context for applying the techniques learned. Compared to the middle school cohort, high school students exhibited deeper inquiry-oriented engagement. Preliminary informal feedback, through observation and a post-event survey, indicated that students appreciated the clarity of the explanations and the level of engagement in learning.

5.3 Use in Community Outreach Activities

Beyond formal workshops, CryptoLearn has been used in broader outreach activities (in the regional library and high school) aimed at increasing awareness of cybersecurity and emerging technologies in the community. During these events, the platform served as both a demonstration tool and an exploratory learning environment, enabling students to engage with cryptographic puzzles and visualize key concepts. Outreach sessions revealed that CryptoLearn's accessible design made it suitable for informal learning environments where participants have varying levels of prior knowledge.

5.4 Observed Engagement and Perceptions

Across all deployment contexts, several consistent patterns emerged:

- High Engagement: Students showed significant interest, especially when interacting with the mystery game and hands-on encryption tools.
- Positive Perceptions: Informal feedback highlighted that students found the explanations approachable and the activities enjoyable.
- Increased Curiosity: Many participants expressed interest in learning more about cybersecurity topics beyond the scope of the workshop.
- Support for Independent Exploration: Students were able to progress through modules without continuous instructor intervention, demonstrating that the interface and explanations were intuitive and self-guided.

6. Conclusion and Future Work

This paper introduced CryptoLearn, a web-based educational platform designed to make cryptography, quantum computing, and post-quantum cryptography accessible to middle school, high school, and early undergraduate students. By combining simplified explanations, visual illustrations, interactive exercises, and a narrative-based mystery game, CryptoLearn supports engagement and conceptual understanding of topics that are traditionally considered abstract and challenging. Deployments in CyberSmart workshops, GenCyber programs, and outreach activities demonstrated positive student perceptions and increased engagement.

The platform’s multi-tier, modular architecture enables extensibility and supports the addition of new learning modules as technologies evolve. While initial deployments provided encouraging insights, future work will focus on conducting structured empirical studies using surveys, interviews, and pre-/post-assessments to evaluate learning outcomes, usability, and motivation. Additional plans include expanding instructional content, enhancing game-based components, and integrating analytics to support classroom use. CryptoLearn aims to serve as a scalable and adaptable model for early cybersecurity and quantum education.

Acknowledgment

This work was supported in part by the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development. For more information about CCI, visit cyberinitiative.org.

References

[1] Sakalli M. T., Bulus E., “Cryptography education for students”, Information Technology Based Proceedings of the Fifth International Conference on Higher Education and Training, ITHET, Istanbul, Turkey, 2004.

[2] Jamshidi A., Kaur K., Gangopadhyay A., “Let students take the wheel: Introducing post-quantum cryptography with active learning”, arXiv Preprint, arXiv:2410.13140, 2024.

[3] Borrelli T. J., Polak M., Radziszowski S., “Designing and delivering a post-quantum cryptography course”, Proceedings of the 55th ACM Technical Symposium on Computer Science Education (SIGCSE), ACM, Portland, OR, USA, 2024.

[4] Abdelhamid S., Patterson S., Patterson B., “Enhancing cryptography education using collaborative visual programming”, Conference Proceedings, The Future of Education 2022, Florence, Italy, 2022.

[5] Yamaguchi K., Kuwana A., Kagami K., “Development of teaching materials for cryptography at senior high school”, Journal of Technology and Social Science 5, no. 1 (2021): 41-46.
[6] Pérez-Ramos É., Caballero-Gil P., “Using GeoGebra to learn the basics of post-quantum cryptography”, Proceedings of the IEEE Frontiers in Education Conference, IEEE, Washington, DC, USA, 2024.
[7] Borrelli T. J., Mishra S., Polak M., Radziszowski S., “A modular approach to teaching post-quantum cryptography”, Proceedings of the 58th ACM technical symposium on computer science education, St. Louis, MO, USA, 2026.
[8] Rao A. R., Dave R., “Developing hands-on laboratory exercises for teaching STEM students the Internet-of-Things, cloud computing and blockchain applications”, Proceedings of the IEEE Integrated STEM Education Conference, IEEE, Princeton, NJ, USA, 2019.
[9] Holden J., “Resource guide for teaching post-quantum cryptography”, Cryptologia, Taylor & Francis, 2023.
[10] Holden J., “Alkaline: A simplified post-quantum encryption algorithm for classroom use”, PRIMUS, Taylor & Francis, 2024.
[11] Abdelhamid S. E., Patterson S., et al., “CryptoQuest: Interactive animation series for teaching cryptography, post-quantum cryptography, and cybersecurity using extended reality (XR)”, Proceedings of the IEEE Frontiers in Education Conference, IEEE, Washington, DC, USA, 2024.