STEM Project Ideas

CRYPTOQUEST: AN EDUCATIONAL GAME ON CRYPTOGRAPHY

Project Description: Develop an interactive game utilizing classical encryption algorithms (Caesar, Vigenère) and modern methods (RSA) to teach high school students about cryptography, integrating STEM skills (Mathematics and Technology).

Technologies Used: Python, JavaScript (Web-based game)

Prepared by: Đỗ Khánh Minh

Mentored by: Nguyễn Phương Hà

TABLE OF CONTENTS

STEM Project Ideas.....1
Background and Context.....2
1. Introduction.....3
1.1. Importance and Challenges of Cryptography.....3
1.2. Objectives of "CryptoQuest".....4
3. Game Structure.....5
3.1. Narrative.....5
3.2. Levels.....5
3.3. Game Mechanics.....6
4. Technology Deployment.....6
5. Implementation Plan.....6
5.1. Phase 1: Research and Design (1-2 Weeks).....6
5.2. Phase 2: Game Development (3-4 Weeks).....6
5.3. Phase 3: Testing and Refinement (1-2 Weeks).....7
6. Expected Outcomes.....7
7. References.....7
Notes.....7

Abstract

Background and Context

Cryptography, the science of securing information through encoding and decoding, has evolved significantly from its historical roots, such as the Caesar Cipher used by Roman emperors, to modern applications like RSA in digital security. Given the projected growth of digital data to 175 zettabytes globally by 2025, as noted in industry reports, the importance of cryptography education is paramount. However, teaching this subject to high school students presents challenges due to its abstract nature, reliance on mathematical concepts like modular arithmetic, and the lack of engaging introductory resources. Traditional methods, such as lectures and textbook exercises, often fail to capture student interest, highlighting the need for innovative approaches like gamified learning.

The "CryptoQuest" project addresses these challenges by leveraging interactive gaming to make cryptography accessible and enjoyable. This aligns with existing educational trends, as evidenced by resources on Teachers Pay Teachers, which offer gamified lesson plans for cybersecurity and cryptography, and academic discussions like those at the University of Washington Math Department, which explore cryptography as a teaching tool for high school students.

1. Introduction

Cryptography, the science of securing information through encoding and decoding, has evolved from a secretive art used by ancient civilizations to a cornerstone of modern digital security. In an era where data breaches, cyber-attacks, and privacy concerns dominate headlines, understanding cryptography is no longer a niche skill reserved for experts—it is a fundamental literacy for the digital age. The "CryptoQuest" project emerges as an innovative educational tool designed to bridge the gap between complex cryptographic concepts and high school learners, leveraging the power of interactive gaming to foster engagement and comprehension. This section outlines the significance of cryptography in today's world, the challenges in teaching it to younger audiences, and the specific objectives of the "CryptoQuest" game.

1.1. Importance and Challenges of Cryptography

Importance of Cryptography

Cryptography plays a pivotal role in safeguarding information across various domains, from online banking and e-commerce to personal communications and national security. Historically, techniques like the Caesar Cipher were used by Roman emperors to protect military messages, while today, advanced algorithms like RSA underpin the security of internet transactions. As of March 26, 2025, the exponential growth of digital data—projected to reach 175 zettabytes globally by 2025 according to industry reports—underscores the urgency of protecting sensitive information. For students, learning cryptography not only introduces them to a critical aspect of cybersecurity but also connects them to real-world applications of mathematics and technology, core components of STEM education. By mastering these concepts, they gain a foundational understanding of how their digital lives are secured, fostering both curiosity and responsibility in an interconnected world.

Challenges in Teaching Cryptography

Despite its importance, teaching cryptography to high school students presents significant hurdles. First, the subject is inherently abstract, relying heavily on mathematical concepts such as modular arithmetic, prime numbers, and exponents—topics that many students find intimidating or disconnected from daily life. Second, traditional classroom methods, such as lectures and textbook exercises, often fail to capture the dynamic nature of cryptography, resulting in low engagement and retention. Third, there is a pedagogical gap: while advanced cryptography is taught at university levels, introductory resources for younger learners are scarce, leaving a void in early STEM education. These challenges highlight the need for an innovative approach that simplifies complex ideas, makes learning interactive, and contextualizes cryptography within a framework that resonates with students' interests, such as gaming.

1.2. Objectives of "CryptoQuest"

The "CryptoQuest" project aims to address these challenges by transforming the way cryptography is introduced to high school students through an interactive, game-based learning experience. The primary objectives of the project are as follows:

- **Educational Empowerment**: To demystify cryptography by breaking down classical algorithms (e.g., Caesar Cipher, Vigenère Cipher) and modern methods (e.g., RSA) into digestible, hands-on lessons embedded within a game narrative. This approach ensures students not only learn how these algorithms work but also why they matter.

- **STEM Integration**: To seamlessly integrate STEM disciplines—specifically mathematics (e.g., modular arithmetic, number theory) and technology (e.g., programming in Python and JavaScript)—into the gameplay, enabling students to apply theoretical knowledge in practical, problem-solving contexts.
- **Engagement and Motivation**: To captivate students' interest through a quest-driven format where they play as adventurers decoding secrets, solving puzzles, and unlocking levels. By gamifying the learning process, "CryptoQuest" seeks to make abstract concepts tangible and enjoyable, fostering a deeper appreciation for STEM.
- **Skill Development**: To cultivate critical thinking, logical reasoning, and basic programming skills as students navigate cryptographic challenges, preparing them for future academic pursuits or careers in fields like cybersecurity and software development.
- **Accessibility**: To create a web-based platform that is widely accessible, requiring only a browser to play, thus ensuring that students and educators from diverse backgrounds can utilize this tool without specialized hardware or software.

Ultimately, "CryptoQuest" aspires to be more than just a game—it is a stepping stone toward building a generation of learners who are confident in their understanding of cryptography and inspired to explore the vast possibilities of STEM. By blending education with entertainment, the project seeks to redefine how complex subjects are taught, making them approachable and relevant to young minds.

2. Game Structure

2.1. Narrative

The player assumes the role of an explorer or secret agent tasked with decoding mysterious messages to prevent a conspiracy or uncover a treasure. Each level introduces a distinct encryption algorithm, progressing from simple (Caesar) to complex (RSA).

2.2. Levels

Level 1: Caesar Cipher

- **Description**: Decode a message encrypted using a shift cipher.
- **Tools**: Players input a "shift key" to attempt decryption.
- **Mathematics**: Basic modular arithmetic (mod 26 for the alphabet).

- **Objective**: Understand simple encryption and decryption processes.

Level 2: Vigenère Cipher

- **Description**: Decode a longer message using a keyword.
- **Tools**: Hints on letter frequency analysis or keyword testing.
- **Mathematics**: Combination of multiple shifts based on the keyword.
- **Objective**: Enhance analytical thinking and comprehension of polyalphabetic ciphers.

Level 3: RSA (Basic)

- **Description**: Decode a numeric message by determining the public and private keys.
- **Tools**: The game provides small prime numbers (p, q) to calculate n and phi(n).
- **Mathematics**: Number theory (prime numbers, Euler's function).
- **Objective**: Introduce the concept of modern asymmetric encryption.

2.3. Game Mechanics

- **Tasks**: Players receive an encrypted message and must decrypt it by entering the solution or selecting appropriate tools.
- **Support**: A hint system explains the algorithm step-by-step if players encounter difficulties.
- **Scoring**: Complete tasks quickly and accurately to earn points, unlocking subsequent levels.

3. Technology Deployment

Version 1: Python (Offline)

- Utilizes a simple library such as tkinter to create a basic graphical interface.
- Encryption and decryption logic is implemented in Python.
- Suitable for classroom use or rapid prototyping.

Version 2: JavaScript (Web Game)

- Employs HTML/CSS to design an aesthetically pleasing interface.
- JavaScript handles game logic and user interaction.
- Deployed on a free web platform (e.g., GitHub Pages) for easy student access.

4. Implementation Plan

4.1. Phase 1: Research and Design (1-2 Weeks)

- Investigate the Caesar, Vigenère, and RSA algorithms (simplified versions).
- Outline the narrative and puzzle designs.
- Determine the primary technology (Python or JavaScript).

4.2. Phase 2: Game Development (3-4 Weeks)

- Program the encryption and decryption algorithms.
- Design the interface and integrate game logic.
- Develop levels with progressively increasing difficulty.

4.3. Phase 3: Testing and Refinement (1-2 Weeks)

- Identify and fix bugs while adjusting difficulty levels.
- Collect feedback from students and mentors for improvement.
- Finalize the gameplay instruction manual.

5. Expected Outcomes

- Students gain an understanding of how basic encryption algorithms function.
- Development of programming and mathematical reasoning skills through practice.
- Creation of a complete product (the game) shareable within the student community.

6. References

- Book: *The Code Book* by Simon Singh (introduction to cryptography).
- Online Resources: Khan Academy (number theory), W3Schools (JavaScript basics).
- Tools: Python.org, CodePen (web game experimentation).

Notes

- The translation retains the hierarchical structure (e.g., 4 with two versions, 5 with three phases) and all specific details.