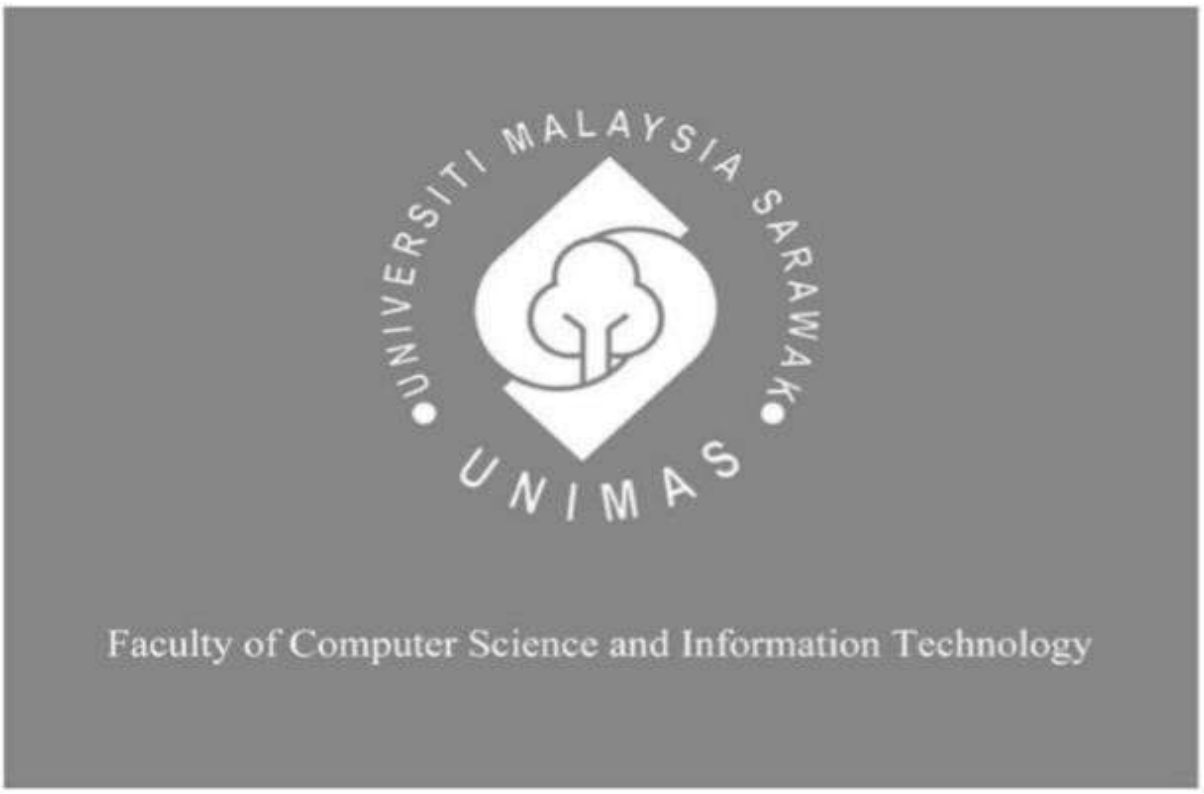


CRYPTO CHRONICA: A GAME-BASED APPROACH TO TEACHING CRYPTOGRAPHY FUNDAMENTALS

EDDRIE RUGU WESTANE

Bachelor of Software Engineering with Honours

(Software Engineering)

2024/2025

CRYPTO CHRONICA: A GAME-BASED APPROACH TO TEACHING CRYPTOGRAPHY FUNDAMENTALS

EDDRIE RUGU WESTANE

This project is submitted in partial fulfilment of

the requirements for the degree of Bachelor of Software Engineering with Honours

(Software Engineering)

Faculty of Computer Science and Information Technology

UNIVERSITI MALAYSIA SARAWAK

2025

Acknowledgements

I would like to express my heartfelt gratitude to my supervisor, Dr. Izzatul Nabila bt Sarbini, for her invaluable guidance and support throughout the development of my final year project. Her insightful feedback and expertise in the field have been instrumental in shaping this project and ensuring its progress in the right direction.

I am profoundly grateful to the Faculty of Computer Science and Information Technology at University of Malaysia Sarawak (UNIMAS) for providing me with the resources, facilities, and technical support necessary for developing this educational game. The learning environment and infrastructure have been crucial in helping me bring this project to fruition.

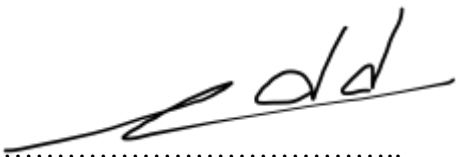
I extend my deepest appreciation to my family for their unwavering support and encouragement throughout this journey. Their patience, understanding, and constant motivation have been my pillar of strength during the challenging phases of this project development.

I am also thankful to my friends and fellow students who have contributed their time and insights during the process of Crypto Chronica. Your feedback and suggestions have helped refine the game's educational aspects and user experience.

Finally, I would like to thank UNIMAS for providing me with this opportunity to pursue my studies and develop this educational game as part of my final year project. The knowledge and experience gained through this journey have been invaluable to my academic and professional growth.

Declaration

I hereby declare that the thesis of Crypto Chronica: A Game-Based Approach To Teaching Cryptography Fundamentals is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that no portion of the work referred in this report has been submitted in support of an application for another degree at University of Malaysia Sarawak (UNIMAS).



……..

Signature

Name: Eddrie Rugu Westane

Matric No.: 77940

Faculty of Computer Science and Information Technology

Abstract

Cryptography has become a part of the digital daily life that goes unnoticed by most. This project proposes a proof-of-concept educational game, Crypto Chronica, to explore the potential of game-based learning in teaching cryptography fundamentals while fostering interest in cybersecurity. The game employs a progression system that mirrors the historical evolution of encryption techniques, making the concepts more accessible to students through a three-phase Learn-Practice-Challenge approach. Through designed gameplay mechanics and puzzle-solving elements, players will learn encryption and decryption techniques including classical ciphers such as substitution and transposition methods, with built-in tools for frequency analysis and pattern recognition. The project will be developed following an iterative approach, incorporating software engineering principles. The expected outcome is a functional prototype that demonstrates how game-based learning can effectively introduce cryptography concepts in an engaging manner. This proof-of-concept aims to establish a foundation for future development of educational games in cryptography education.

Abstrak

Kriptografi telah menjadi sebahagian daripada kehidupan digital harian yang sering tidak disedari oleh kebanyakan orang. Projek ini mencadangkan satu permainan pendidikan bukti konsep, Crypto Chronica, untuk meneroka potensi pembelajaran berasaskan permainan dalam pengajaran asas kriptografi sambil memupuk minat dalam keselamatan siber. Permainan ini menggunakan sistem perkembangan yang mencerminkan evolusi sejarah teknik penyulitan, menjadikan konsep-konsep lebih mudah difahami oleh pelajar melalui pendekatan tiga fasa Belajar-Praktik-Cabaran. Melalui mekanik permainan dan elemen penyelesaian teka-teki yang direka, pemain akan mempelajari teknik penyulitan dan penyahsulitan termasuk sifer klasik seperti kaedah penggantian dan transposisi, dengan alat analisis frekuensi dan pengecaman corak yang tersedia. Projek ini akan dibangunkan mengikut pendekatan lelaran, menggabungkan prinsip-prinsip kejuruteraan perisian. Hasil yang dijangka ialah prototaip berfungsi yang menunjukkan bagaimana pembelajaran berasaskan permainan boleh memperkenalkan konsep kriptografi secara berkesan dan menarik. Bukti konsep ini bertujuan untuk membentuk asas bagi pembangunan masa hadapan permainan pendidikan dalam pendidikan kriptografi.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

1.1 Background

The digital age has made cryptography an essential tool of daily life, from secure messaging to online banking. However, teaching and learning cryptography remains a challenge in an educational setting. Traditional teaching methods often struggle to convey these complex concepts effectively, leading to reduced engagement and understanding among those learning it.

Educational games or game-based learning have emerged as powerful tools for teaching complex subjects by providing interactive, engaging environments where learning occurs naturally through gameplay. Games like “Cypher” have demonstrated the potential of this approach in teaching. This project builds upon these successes by creating an engaging educational game for cryptography fundamentals.

The use of historical context in teaching provides concreate examples of how encryption techniques evolved and why they were necessary. By incorporating this historical progression into a game format, learners can better understand the technical aspects and the significance of the concepts and the roles they played in history.

1.2 Problem Statement

The following challenges have been identified:

1. Traditional teaching methods often present cryptography concepts in an abstract manner, making it difficult for beginners to grasp fundamental principles.
2. Existing educational resources typically lack interactive elements and game-based learning approaches that could help reinforce learning through practical application.

3. Students often struggle to maintain engagement with cryptography concepts due to the theoretical nature of conventional teaching methods and limited hands-on practice.
4. There is a limited availability of well-designed educational games specifically targeting cryptography concepts.

1.3 Objectives

1. To develop a game prototype that teaches cryptography concepts through a historically grounded progression system.
2. To develop an effective learning system within the game that incorporates tutorial mechanisms, progressive difficulty scaling, and interactive puzzle-solving elements.
3. To create an interactive learning framework that teaches cryptographic fundamentals through game mechanics, measuring effectiveness through user completion data, and successful application of concepts in challenge scenarios.

.

1.4 Brief Methodology

The project will follow an iterative development approach. The planning phase will begin with research into existing educational games and cryptography teaching methods, studying successful game-based learning implementations to define appropriate game mechanics that align with the learning objectives.

In the development phase, core game mechanics will be implemented with a focus on learning outcomes. This includes creating a tutorial system with scaffolding learning techniques and developing cryptography puzzles that balance entertainment with educational value. Feedback mechanisms and achievement systems will be integrated to support the learning process.

The testing phase will involve conducting tests that focus on both gameplay and learning aspects. Through iterative feedback and refinement, the game will be optimized to achieve an effective balance between entertainment value and educational objectives.

1.5 Scope

The scope of the project encompasses:

1. Educational Content:
    a. Core cryptography concepts
        i. Basic encryption and decryption principles
        ii. Classical substitution-based ciphers
        iii. Frequency analysis and pattern recognition
        iv. Code breaking fundamentals and techniques
    b. A level or two covering each concept progressively
    c. Historical context integration

2. Game implementation:
    a. Tutorial system for each core mechanism of a level
    b. Level-based progression system
    c. Puzzle-solving interface
    d. Progress tracking functionality
3. Technical:
    a. 2d game engine implementation
    b. Single player experience
    c. Desktop platform
4. Learning Assessment Features:
    a. In-game progress tracking
    b. Level completion metrics
    c. Basic performance feedback

1.6 Significance of Project

The development of Crypto Chronica represents an exploration into the potential of game-based learning for cryptography education. As a proof-of-concept, this project investigates how interactive gameplay can serve as an alternative teaching tool for cryptography concepts. By demonstrating how complex cryptographic principles can be made more accessible to beginners through game mechanics, the project provides valuable insights into the effectiveness of interactive learning approaches in technical education.

From a practical perspective, the project serves as a test case for integrating game-based learning into cryptography education. The prototype demonstrates how technical concepts can be taught through interactive engagement, providing a model that can inform future educational game development. Additionally, the project's framework and findings will contribute to the understanding of how educational games can be effectively designed for teaching complex technical subjects.

The project's significance is further enhanced by its timing, as the need for cybersecurity education continues to grow in our increasingly digital world. By exploring an engaging approach to introducing cryptographic concepts, this proof-of-concept helps pave the way for innovative methods of preparing students for further study in cybersecurity while developing their problem-solving skills through practical application of cryptographic principles.

1.7 Project Schedule

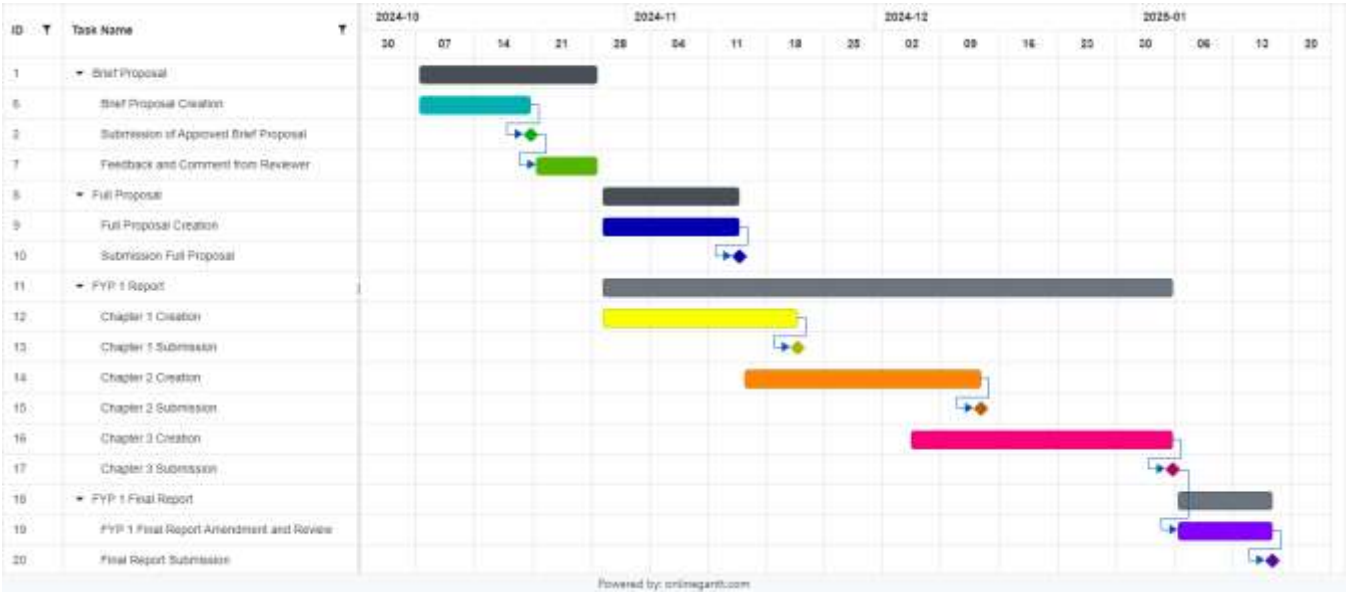


Figure 1.1: Project Schedule Gantt Chart

1.8 Expected Outcome

The project deliverables are:

1. A functional game prototype featuring:
    a. A tutorial system
    b. Three or more levels covering different encryption techniques
    c. Interactive puzzle-solving mechanics
    d. Progress tracking system

The expected outcome of the project is to deliver a functional game prototype featuring three or more levels covering different encryption techniques, interactive puzzle-solving mechanics using cryptography and progress tracking.

1.9 Project Outline

The project is outlined in the following:

Chapter 1: Introduction

This chapter presents an introduction to the project concept and establishes its foundational elements. The chapter introduces the background of cryptography education and the potential of game-based learning in this domain. It identifies the key challenges in traditional cryptography education through the problem statement and sets clear objectives for the development of an educational game solution. Additionally, this chapter outlines the project scope and provides a brief description of the methodology that will guide the development process. The chapter concludes by highlighting the project's significance and describing the expected outcomes.

Chapter 2: Literature Review

This chapter provides a comprehensive literature review examining existing educational games and similar works in the field. This chapter explores current research on game-based learning effectiveness, with particular focus on cybersecurity education. The chapter presents detailed analyses of similar games including Cypher, Keep Talking and Nobody Explodes, and CryptoClub, examining their features, approaches, and limitations. Through this review, the chapter identifies gaps in current solutions and areas where Crypto Chronica can innovate.

Chapter 3: Requirement Analysis and Design

This chapter details the requirement analysis and design specifications for the project implementation. This chapter outlines the development methodology and presents both functional and non-functional requirements for the game. It provides comprehensive use case analyses, interface design specifications, and detailed gameplay mechanics. The chapter describes the learning progression system and presents the implementation plan, including development phases and testing strategies. Through these specifications, the chapter establishes the technical foundation for the game's development.

Chapter 2: Literature Review

2.1 Introduction

The development of an educational game for teaching cryptography requires an understanding of existing solutions and available technologies. This chapter will review works similar to that of the project and the technical tools relevant to the project's implementation.

Research has shown that game-based learning is effective across various subjects. A study by Shakhmalova & Zotova (2023) demonstrated significant improvement in student performance and increased motivation in learning English grammar compared to traditional teaching methods. This effectiveness extends to STEM education, where a comprehensive meta-analysis by Gui et al. (2023) revealed that digital game-based STEM learning showed a medium to large general effect (g=0.624) compared to traditional STEM learning methods. Their analysis of 136 effect sizes from 86 studies found that game-based learning was particularly effective for developing cognitive skills compared to knowledge acquisition.

Jin et al. (2018) evaluated game-based learning approaches for teaching cybersecurity concepts to high school students and found through survey data that the method was very effective in cybersecurity awareness training. Their study highlighted that well-designed educational games could make complex cybersecurity concepts more accessible to students of varying ability levels.

More recently, Tharot et al. (2024) demonstrated the effectiveness of gamification in cybersecurity education through role-play-based scenarios. Their study with 51 students found that over 90% of participants would recommend game-based learning approaches, with 88.2% rating their experience as good or excellent. This provides further evidence that well-designed educational games can effectively teach complex cybersecurity concepts to students of varying backgrounds.

The first section of this chapter examines existing educational games that either teach cryptography or demonstrate effective approaches to teaching technical concepts through gameplay. By analysing these games, valuable insights can be gleaned about effective teaching methods, engagement mechanisms, and potential areas for improvement. This analysis will inform the design decisions for Crypto Chronica, ensuring it builds upon effective approaches while addressing identified gaps.

2.2 Review on Similar Works

This section reviews various games that provide insight for the development of Crypto Chronica. The works selected for review include purpose-built educational games and commercial games with strong puzzle or cryptography elements. Each game is analysed for its educational approach, engagement mechanics, and features related to teaching cryptography concepts.

2.2.1 Cypher

Cypher, developed by Matthew Brown in 2018 (Cypher on Steam, n.d.), is an educational puzzle game designed to teach cryptographic concepts through an art gallery-themed environment. The game was developed as a first-person puzzle game about cryptography. It is set in a minimalist gallery setting, players encounter various cryptography puzzles each accompanied by its history and text explaining its underlying concepts.

The game implements a progressive learning approach where players advance through different rooms, each focusing on a specific cryptographic concept and is tasked with deciphering the message. While the game succeeds in presenting the concepts in an aesthetically pleasing environment, it faces challenges in bridging the gap between theoretical explanation and practical applications.

The player is first introduced to the theory with its explanatory texts, then to use that theory to solve the cipher and obtain the hidden message. The game fails in showing an example of the theory in action. If players were to get stuck on a cipher, they will be stuck. The game does provide a hint for the cipher; however, it lacks in assisting the player to a way to solve it.

Figure 2.1: Explanatory text explaining the concept

The game also expects the player to have a pen and paper ready in order to solve the cipher, which highlights the game's potential limitations especially towards certain puzzles. Some puzzles are particularly long that what is ideal may be to make notes where the puzzle is rather than having to transcribe the puzzle onto a piece of paper which makes it tedious.

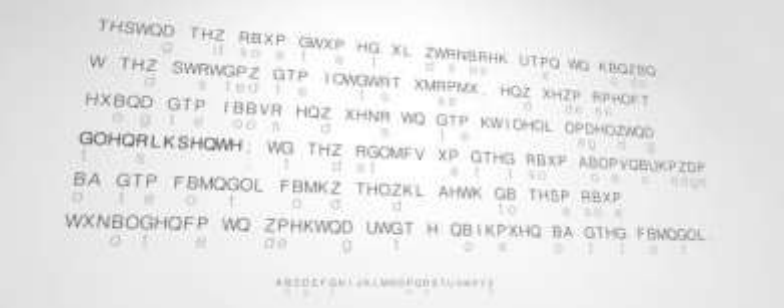


Figure 2.2: A cipher to be solved

Analysis of the game revealed both strengths and weaknesses in its approach. The game's clean interface and structured progression provides a scaffolding for its player to learn the concepts and solve the ciphers, however, some players may find the difficulties in transitioning from theory to practical difficult without some more assistance. This suggests a need for application when explaining the theory in order to adequately teach the concept. The game also lacks some user-friendliness with the lack interacting with the puzzle with having to resort to transcribing the puzzle onto paper.

2.2.2 Keep Talking and Nobody Explodes

Keep Talking and Nobody Explodes is developed by Steel Crate Games in 2015 (Keep Talking and Nobody Explodes, 2023), it represents an innovative approach to puzzle-solving through asymmetric multiplayer gameplay. While not explicitly designed as an educational tool, its core mechanics demonstrate valuable principles for teaching problem-solving and ciphers that are relevant to cryptography education.

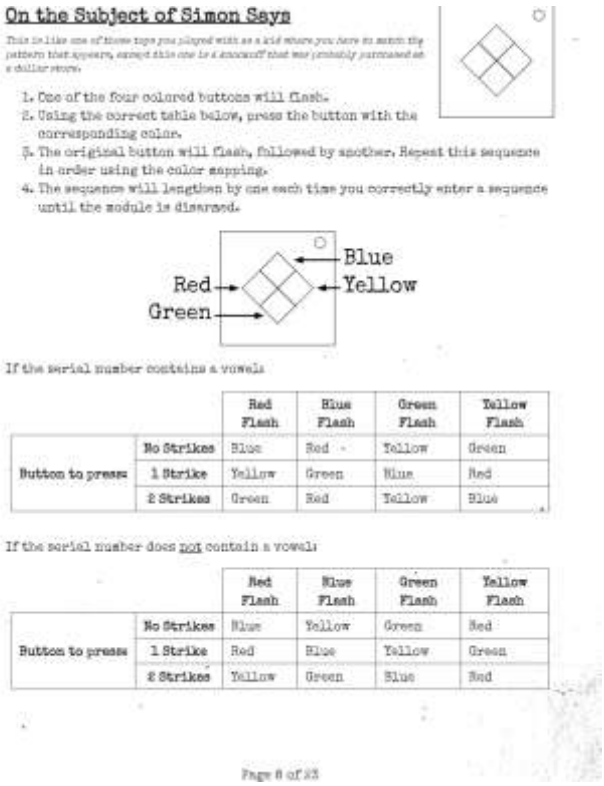
The game implements a unique information-sharing mechanic where one player interacts with a virtual bomb while others consult a manual containing decryption instructions. This separation of information creates a scenario where understanding encoded information requires both technical knowledge and systematic problem-solving approaches.

The game's value lies in its approach to teaching pattern recognition and code interpretation. Players must quickly learn to understand and communicate complex symbols, sequences, and patterns under time pressure. The manual's structured approach to presenting information also provides insights into how technical documentation can be organized for learning purposes.

Figure 2.3: Virtual Bomb

The primary game mechanics to be considered relevant to the project's design includes:

- Progressive difficulty through increasingly complex modules
- Immediate feedback through visual audio cues
- Engagement through time pressure and collaborative problem-solving



On the Subject of Simon Says

1. One of the four colored buttons will flash.
2. Using the correct table below, press the button with the corresponding color.
3. The original button will flash, followed by another. Repeat this sequence in order using the color mapping.
4. The sequence will lengthen by one each time you correctly enter a sequence until the module is disarmed.

Red
Blue
Yellow
Green

If the serial number contains a vowel:

		Red Flash	Blue Flash	Green Flash	Yellow Flash
Button to press:	No Strikes	Blue	Red	Yellow	Green
	1 Strike	Yellow	Green	Blue	Red
	2 Strikes	Green	Red	Yellow	Blue

If the serial number does not contain a vowel:

		Red Flash	Blue Flash	Green Flash	Yellow Flash
Button to press:	No Strikes	Blue	Yellow	Green	Red
	1 Strike	Red	Blue	Yellow	Green
	2 Strikes	Yellow	Green	Blue	Red

Figure 2.4: An excerpt of the manual

However, the game also presents limitations when considered as an educational tool. Its focus on entertainment over explicit teaching means that players may not fully grasp the underlying concepts as the answer are presented in the manual. The time pressure, while engaging may be a con, such that it could potentially hinder deep learning of complex concepts. Additionally, the game is limited as an educational tool with its emphasis on speed over methodical understanding.

2.2.3 CryptoClub

CryptoClub, developed as an educational web platform by the University of Chicago (CryptoClub, n.d.), represents a direct approach to teaching cryptography through interactive online tools and games. The platform was specifically designed to introduce young learners to fundamental cryptography concepts through a combination of structured lessons and games.

The platform employs a comprehensive educational approach by integrating various learning tools. Users encounter different types of ciphers through interactive exercises, starting with basic substitution ciphers to increasingly complex encryption methods such as the Vigenère cipher. The concepts are taught by an educator with access to the manual provided by the platform.

Figure 2.5: Homepage of CryptoClub

CryptoClub's is designed with a focus on immediate practical application. Each cryptographic concept is presented with interactive tools that allow students to both encrypt and decrypt messages, providing hands-on experience with the principles being taught. This approach helps bridge the gap between theoretical understanding and practical application.

Figure 2.6: A Challenge

However, the platform is clearly aimed at young learners with a focus on improving not just an understanding of fundamental cryptography concepts but also their math skills. The concepts taught are limited to particularly substitution ciphers. The platform itself is quite limited in terms of its engagement features and its web-based structure may be limiting its functionality.

2.2.4 Comparison of Features

Analysis of Cypher, Keep Talking and Nobody Explodes, and CryptoClub reveals different approaches to educational game design and engagement mechanisms. While each work serves different primary purposes, their features and limitations provide valuable insights for developing effective educational games.

2.2.4.1 Features Comparison

1. Teaching Approaches

Each work demonstrates distinctive methods of conveying information and engaging users. Cypher utilizes a museum-style first-person presentation with progressive puzzle rooms, focusing on self-directed learning through explanatory texts and ciphers to solve. Keep Talking and Nobody Explodes, though not typically considered educational, presents itself as an engaging way to solve problems collaboratively. CryptoClub takes a structured educational approach, combining mathematical principles with cryptography through guided activities and games.

2. User Engagement Methods

The works employ varying strategies to maintain user interest. Cypher creates engagement through its aesthetic environment and puzzle progression. Keep Talking and Nobody Explodes generates excitement through time pressure and social interaction. CryptoClub focuses on practical application and collaborative activities, emphasising learning through doing.

3. Learning Effectiveness

Each work presents different strengths in its value as an educational tool. Cypher excels presenting complex concepts in an accessible format but struggles with the transition of theory-to-practice. Keep Talking and Nobody Explodes effectively teaches pattern recognition and

problem solving however its emphasis on speed may find itself lacking in value as an educational tool despite its engagement. CryptoClub provides structured learning but may lack immersive qualities of modern educational games and its limited content is aimed at a younger audience

2.2.4.2 Comparative Analysis Summary

Table 2.1: Table of Comparison

Feature	CryptoClub	Cypher	Keep Talking and Nobody Explodes
Primary Purpose	Educational platform for teaching cryptography and mathematics	Educational game focused on cryptography concepts	Entertainment game with puzzle-solving and communication elements
Target Audience	Middle school students and educators	General audience interested in cryptography	General gaming audience
Teaching Method	Structured curriculum with hands-on activities and games	Self-guided exploration through puzzle rooms	Indirect learning through collaborative problem-solving
Progression System	Curriculum-based progression with flexible implementation	Room-based progression with increasing puzzle complexity	Module-based progression with increasing difficulty
Feedback Method	Teacher-guided feedback and built-in assessment tools	Console-based answer validation and hints	Real-time feedback through game mechanics and time pressure
Key Strengths	- Flexible implementation	- Clean, focused design	- Strong engagement

	- Structured learning approach - Collaborative activities	- Progressive difficulty - Aesthetic presentation - Comprehensive cryptography coverage	- Immediate feedback -Effective pattern recognition
Limitations	- Basic interface - Limited gamification - Requires external facilitation - Limited concepts aimed at younger audience	- Steep learning curve - Limited interactive tools - Requires external notetaking - Gap between theory and practice	- Not explicitly educational - High pressure environment - Limited depth in cryptography - Speed over understanding

2.2.4.3 Project Analysis

The analysis of Cypher, Keep Talking and Nobody Explodes, and CryptoClub reveals crucial insights that inform the development of Crypto Chronica. The review demonstrates a clear need for an educational game that effectively bridges the gap between theoretical understanding and practical application of cryptographic concepts, which existing solutions have not fully addressed.

Crypto Chronica aims to combine the structured learning approach of CryptoClub with the engaging gameplay mechanics of Keep Talking and Nobody Explodes, while improving upon the theory-to-practice transition that Cypher struggles with. From CryptoClub, the project will adopt the hands-on approach to learning cryptographic concepts but enhance it with more sophisticated game mechanics and a broader range of cryptographic topics. The engagement mechanics of Keep Talking and Nobody Explodes inspire the implementation of immediate feedback systems and progressive difficulty scaling, though without the potentially overwhelming time pressure.

The project will specifically address the limitations identified in existing solutions. Unlike Cypher, which requires external notetaking, Crypto Chronica will incorporate built-in tools for working with ciphers. The project will expand beyond CryptoClub's basic interface and limited concept range, offering a more comprehensive coverage of cryptography topics with modern gaming elements. To improve upon the existing solutions, the project will:

1. Implement an interactive workspace for cipher manipulation, eliminating the need for external tools.
2. Create a balanced progression system that introduces concepts gradually while maintaining engagement.

3. Develop comprehensive tutorials that demonstrate practical applications of theoretical concepts.
4. Include varied feedback mechanisms that guide learning without inducing excessive pressure.
5. Design engaging gameplay mechanics that naturally reinforce learning objectives.

These improvements draw from the strengths of existing solutions while addressing their identified limitations, positioning Crypto Chronica as an effective tool for cryptography education.

2.3 Foundational Cryptography

Classical cryptography serves as the foundation for understanding modern security systems, with Caesar and substitution ciphers providing essential pedagogical bridges between mathematical theory and practical security applications (Cohen & Kahn, 1997). These fundamental encryption methods demonstrate core cryptographic principles while maintaining sufficient simplicity for educational implementation.

2.3.1 Historical Development and Origins

The earliest documented cryptographic practices emerged in ancient Egypt around 1900 BC, where scribes employed non-standard hieroglyphs carved into tomb walls to conceal sensitive information (Singh, 1999). Mesopotamian civilizations utilized similar techniques on clay tablets circa 1500 BC to protect commercial information, particularly ceramic glaze formulations. These early implementations established the fundamental concept of deliberate information concealment through systematic symbol manipulation.

Greek civilizations advanced cryptographic thinking through mechanical devices and systematic approaches. The Scytale, employed by Spartans around 650 BC, utilized transposition through leather strips wrapped around wooden staffs of specific dimensions. Polybius developed a grid-based substitution system (c. 200-118 BC) that encoded letters into numerical pairs, demonstrating early understanding of both substitution and transposition principles that remain central to modern cryptographic design (Simmons & J, 2025).

2.3.2 Caesar Cipher Implementation and Properties

Roman historian Suetonius documented Julius Caesar's systematic use of a substitution cipher employing a consistent three-position alphabet shift during the Gallic Wars (60-44 BC). This cipher replaced each letter with the character three positions later in the Latin alphabet, proving

effective against contemporary enemies who lacked both literacy and systematic cryptanalytic methods (Wikipedia contributors, 2025).

The Caesar cipher operates using modular arithmetic in Z_{26}, with encryption function $E(x) = (x + k) \bmod 26$ and decryption function $D(x) = (x - k) \bmod 26$, where x represents plaintext letters (0-25) and k denotes the shift key. This transformation demonstrates bijective properties ensuring reversibility and forms a mathematical group under composition (Savarese & Hart, 2010). However, the cipher exhibits critical vulnerabilities including an extremely limited key space of only 25 possible keys, representing approximately 4.64 bits of entropy.

2.3.3 Substitution Cipher Evolution and Mathematical Complexity

General substitution ciphers represent mathematical generalizations of Caesar's approach, employing arbitrary alphabet permutations rather than systematic shifts. Where Caesar utilizes $\pi(x) = (x + k) \bmod 26$, general substitution implements arbitrary mappings $\pi(x) =$ permutation. This expansion creates a dramatically larger key space of $26! \approx 4.03 \times 10^{26}$ possible keys, representing approximately 88.4 bits of entropy and a substantial increase over Caesar cipher security (Dave, 2024).

The mathematical complexity increase provides apparent security improvements, yet substitution ciphers remain vulnerable to statistical analysis. Modern research demonstrates that computational approaches using genetic algorithms achieve reliable success in key recovery for simple substitution ciphers (Spillman et al., 1993).

2.4 Cryptanalytic Techniques and Vulnerabilities

2.4.1 Frequency Analysis Development

Al-Kindi's revolutionary work (c. 850 CE) fundamentally undermined monoalphabetic substitution cipher security through systematic frequency analysis. Working at Baghdad's House of Wisdom, Al-Kindi authored the first comprehensive treatise on cryptanalysis, developing methods for analyzing letter frequency patterns in natural languages and matching these patterns to break substitution ciphers Telsy (2022). This breakthrough marked the transition from the first era of cryptography to systematic cryptanalytic science.

Frequency analysis exploits fundamental linguistic statistics where English letters appear with characteristic frequencies: E (12.7%), T (9.85%), A (8.12%). The technique requires sufficient ciphertext length, typically 25-27 characters for English, as established through Shannon's entropy calculations. Modern implementations employ chi-squared statistical analysis comparing observed frequency distributions in ciphertext with expected language distributions using $\chi^2 = \Sigma[(\text{observed} - \text{expected})^2/\text{expected}]$ (101Computing, 2024).

2.4.2 Historical Cryptanalytic Applications

The Babington Plot (1586) exemplifies the practical consequences of cryptographic vulnerabilities. Mary, Queen of Scots, and conspirator Anthony Babington employed a nomenclator cipher combining 23 alphabet symbols, 35 word/phrase symbols, and null characters. Sir Francis Walsingham's intelligence operation successfully utilized Thomas Phelippes to break the cipher using Al-Kindi's frequency analysis techniques developed seven centuries earlier. The decrypted communications provided explicit evidence of treason, directly leading to Mary's execution (The Babington Plot, 2024).

This historical example demonstrates both the practical application of cryptanalytic theory and the fatal consequences of overconfidence in cryptographic security. The case illustrates how

mathematical vulnerabilities translate into real-world security failures when cryptographic systems fail to account for statistical properties of natural language.

2.5 Development Tools

The game will be developed using the Godot game engine, chosen for its lightweight nature, robust 2D capabilities, and cross-platform support (Linietsky et al., 2024). Godot's node-based architecture aligns well with the modular design requirements of educational games, allowing for flexible component development and easy integration of new features. The engine's built-in scripting language, GDScript, provides sufficient functionality for implementing cryptographic algorithms while maintaining development efficiency.

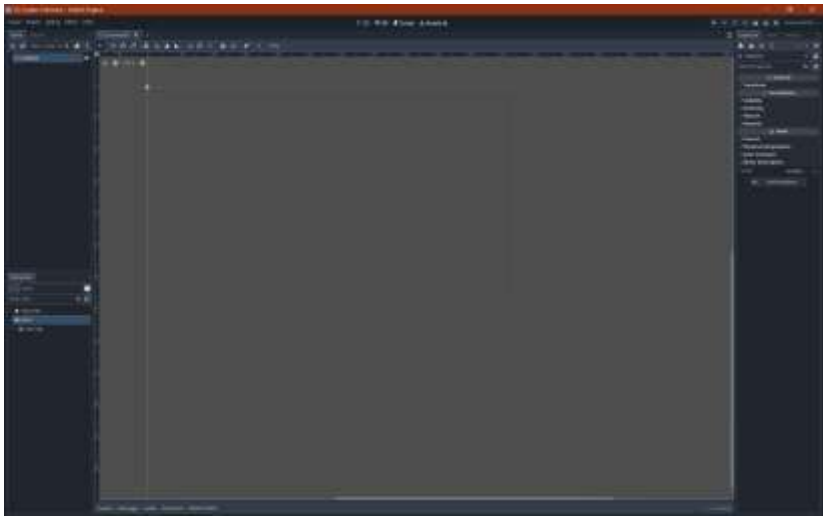


Figure 2.7: Development Environment Overview for 2D Games

For graphics and asset creation, Aseprite will be used as the primary pixel art and animation tool. Aseprite's specialized features for pixel art creation, including advanced animation tools and precise sprite editing capabilities, make it ideal for developing the game's 2D assets. The tool's ability to export sprite sheets and animation files in formats compatible with Godot ensures smooth integration of visual assets into the game.

Version control is implemented using Git to support the iterative development process and maintain a history of changes. The repository follows a simple branching structure where the

main branch contains stable versions of the game, with separate branches created for developing and testing new features. This approach ensures that there is always a working version of the game while new components are being developed and tested.

The selected tools provide a balance between development efficiency and required functionality for game development. Godot's integrated development environment (IDE) includes built-in debugging tools and scene management features that facilitate rapid prototyping and testing of game mechanics. These capabilities are essential for implementing and refining the educational and gameplay elements of Crypto Chronica.

2.6 Summary

This chapter established the theoretical foundation and contextual framework for developing Crypto Chronica as an educational cryptography game. The literature review demonstrated that game-based learning approaches show significant effectiveness in STEM education, with studies revealing medium to large effect sizes compared to traditional teaching methods. The analysis of existing educational games revealed critical gaps in current solutions, particularly in bridging the theory-to-practice transition that students require for deep understanding of cryptographic concepts.

The comparative analysis of Cypher, Keep Talking and Nobody Explodes, and CryptoClub identified key strengths and limitations that inform the project's design decisions. While Cypher provides comprehensive cryptographic coverage, it lacks interactive tools and practical application guidance. CryptoClub offers structured learning but remains limited in scope and engagement. Keep Talking and Nobody Explodes demonstrates effective engagement mechanics but prioritizes speed over methodical understanding. These findings highlight the need for an educational game that combines structured learning approaches with engaging gameplay mechanics while providing comprehensive interactive tools for cipher manipulation.

The examination of foundational cryptography concepts, from ancient Egyptian practices to Al-Kindi's frequency analysis, establishes the historical context and mathematical principles that underpin the educational content. Understanding these classical techniques and their vulnerabilities provides the pedagogical foundation necessary for students to appreciate both the evolution of cryptographic thinking and the mathematical principles that drive modern security systems.

The selected development tools—Godot game engine, Aseprite for asset creation, and Git for version control—provide a robust foundation for implementing the identified design requirements. These tools offer the necessary capabilities for creating an interactive educational experience while maintaining development efficiency and cross-platform compatibility essential for educational deployment.

Chapter 3: Requirement Analysis and Design

3.1 Introduction

Software development methodology plays a crucial role in game development, particularly for educational games where user feedback and iterative improvement are essential for achieving both entertainment and learning objectives. This chapter outlines the development approach, requirements, design decisions, and implementation strategy for Crypto Chronica, an educational game aimed at teaching cryptography concepts through interactive puzzles.

The decision to adopt an iterative development approach stems from the unique challenges of educational game development. Educational games must balance entertainment value with learning effectiveness, requiring frequent testing and refinement based on user interaction and learning outcomes. This iterative approach allows for continuous improvement of both gameplay mechanics and educational content based on user feedback and testing results.

This chapter is structured to provide a comprehensive overview of the development process, beginning with the methodology, progressing through requirements analysis and game design, and concluding with the technical architecture and implementation plan. Each section builds upon the previous ones to create a cohesive development strategy that addresses both the technical and educational aspects of the game.

3.2 Development Methodology

3.2.1 Iterative Development Approach

The development of Crypto Chronica follows an iterative approach, characterized by short development cycles focused on specific features or components. Each iteration cycle consists of four main phases: planning, implementation, testing, and evaluation. This approach allows for rapid prototyping and refinement of game mechanics based on user feedback and learning effectiveness assessment.

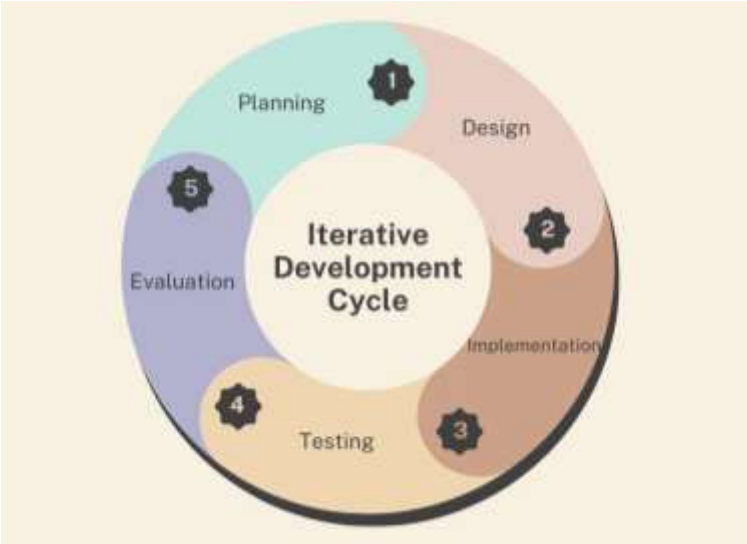


Figure 3.1: Iterative Development Cycle

During the planning phase, objectives for the current iteration are defined based on previous feedback and the overall project roadmap. Implementation focuses on developing or refining specific features, followed by internal testing to verify functionality. The evaluation phase involves user testing and feedback collection, with results informing the planning of subsequent iterations.

Feature implementation follows a progressive pattern, starting with core mechanics and gradually adding complexity. This approach ensures that fundamental systems are robust before building more advanced features upon them. Early iterations focus on basic cipher

mechanics and user interface elements, while later iterations introduce more complex cryptographic concepts and advanced learning features.

The feedback integration process is structured to capture both technical and educational aspects. Technical feedback addresses gameplay mechanics and user interface issues, while educational feedback focuses on learning effectiveness and concept comprehension. This dual feedback approach ensures that both entertainment and educational objectives are met through each iteration.

3.3 Requirements Analysis

The requirements for Crypto Chronica have been derived from project objectives, analysis of similar works, and the need to create an effective educational game. These requirements are categorized into functional requirements that define specific system capabilities and non-functional requirements that specify quality attributes and constraints.

3.3.1 Functional Requirements

The functional requirements encompass four core areas essential to meeting the project's educational and gameplay objectives:

3.3.1.1 Educational Content Requirements

The system must provide comprehensive cryptographic education through historical context, interactive demonstrations, and practical applications. Historical narratives must accompany each cipher type, supported by interactive demonstrations that clearly illustrate encryption techniques. The educational content must accommodate multiple learning styles through textual explanations, visual demonstrations, and hands-on practice opportunities.

3.3.1.2 Learning Progression Requirements

A structured learning path must guide users through cryptographic concepts with increasing complexity. The progression system must track user advancement, manage prerequisites for advanced content, and ensure concept mastery before progression. The system must identify when users struggle with concepts and provide appropriate remedial content to support their learning journey.

3.3.1.3 Interactive Tool Requirements

The system must implement a comprehensive set of built-in cryptographic tools supporting both learning and puzzle-solving activities. These tools include cipher wheels, frequency analysis tools, and pattern recognition aids. Tool availability must align with concept introduction, accompanied by clear usage instructions and contextual guidance.

3.3.1.4 Feedback and Assessment Requirements

Immediate and clear feedback must be provided for all user actions and progress. The system must validate puzzle solutions, provide contextual hints when needed, and maintain detailed performance metrics. Feedback mechanisms must offer constructive guidance for struggling users while maintaining engagement through appropriate challenge levels.

3.3.2 Non-Functional Requirements

3.3.2.1 Performance Requirements

The system must maintain responsive performance on standard desktop computers. This includes immediate response to user interactions, level transitions completing within three seconds, and efficient resource utilization to ensure smooth operation on typical hardware configurations.

3.3.2.2 Usability Requirements

The user interface must prioritize clarity and ease of use. All game elements and instructions must be clearly visible and readable. New features and tools must be introduced gradually with appropriate tutorials. The system must prevent invalid inputs and provide clear error messages, while allowing users to undo actions and restart puzzles without losing progress.

3.3.2.3 Educational Design Requirements

The game must maintain user engagement through varied challenges and meaningful rewards. Learning materials must build upon previously introduced concepts in a logical progression. The system must accommodate different learning speeds and styles while providing unobtrusive but informative progress tracking.

3.3.2.4 Technical Requirements

The game must operate reliably on standard desktop operating systems. User progress must be automatically saved and recoverable. The system must handle invalid inputs gracefully without crashing, and the underlying code structure must support future expansion with additional cipher types and puzzles.

These requirements establish the foundation for developing Crypto Chronica as an effective educational tool while ensuring technical reliability and user engagement.

3.3.3 Use Cases

3.3.3.1 Use Case Overview

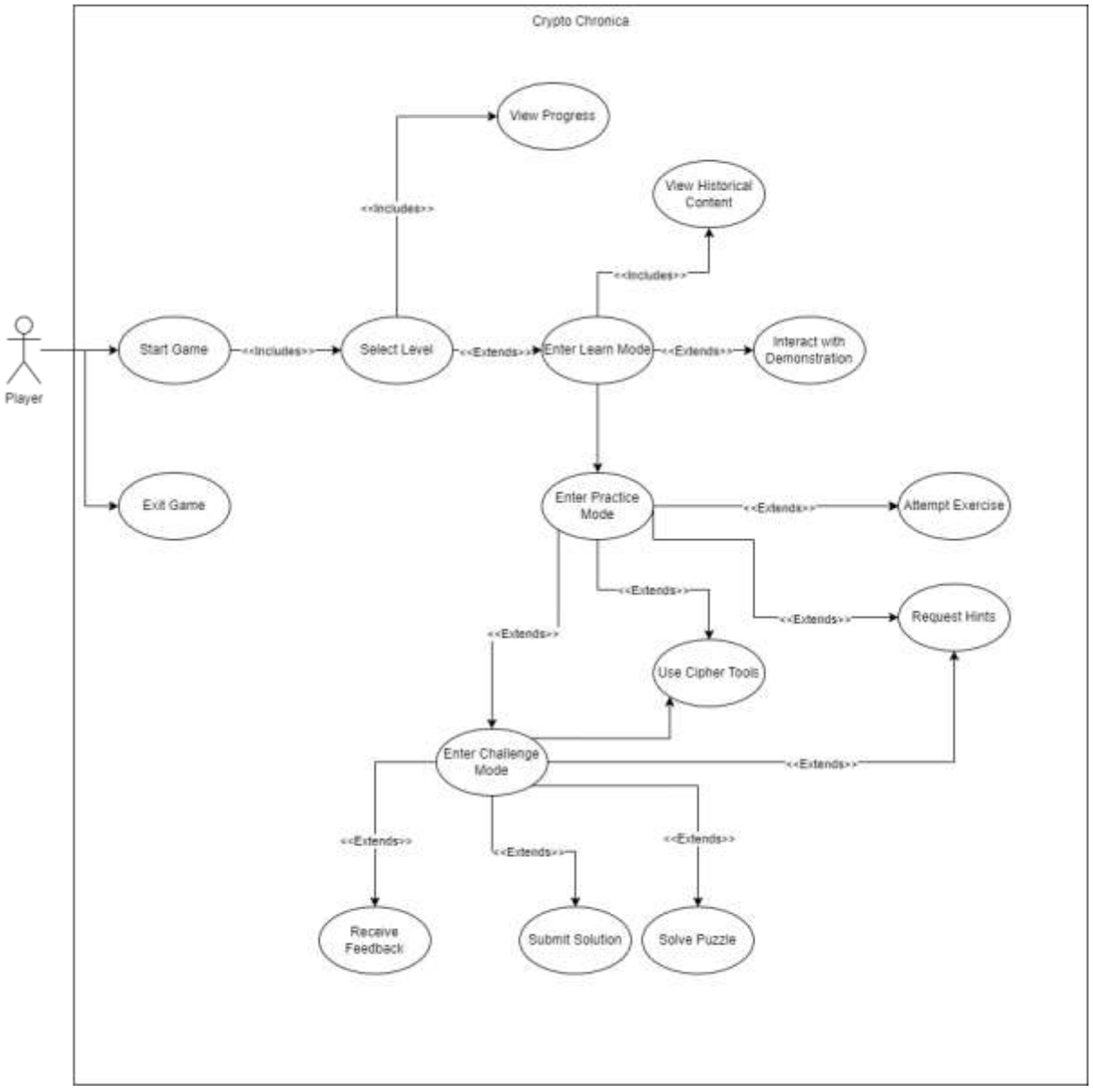


Figure 3.2: Crypto Chronica Use Case Diagram

Figure 10 presents the use case diagram for Crypto Chronica, illustrating the main interactions between the player and the game system. The diagram captures the core gameplay loop and learning progression system described in the game design.

The system's main entry point begins when a player starts the game, leading to level selection where they can view their progress across different cipher types. From level selection, players

enter the learning progression system that consists of three main modes: Learn, Practice, and Challenge.

In Learn Mode, players can view historical content about the cipher and interact with demonstrations to understand the encryption concepts. Practice Mode extends the learning experience by allowing players to attempt exercises using cipher tools, with optional hint support. Challenge Mode represents the final phase where players apply their knowledge to solve puzzles and submit solutions, receiving feedback on their performance.

3.3.3.2 Detailed Use Case Description

3.3.3.2.1 Start Game

Actors:

- Player

Goal:

- To initialize the game and access the level selection interface

Preconditions:

- Game application is successfully launched

Postconditions:

- Player is presented with the level selection interface
- Game state is initialized

Main Flow:

1. Player launches the game application
2. System loads necessary game assets
3. System displays the main menu
4. Player selects "Start Game" option
5. System transitions to level selection interface

Alternative Flow:

- If a previous save exists, system offers option to continue from last save point

Exceptions:

- If game assets fail to load, system displays error message and returns to main menu

3.3.3.2.2 Select Level

Actors:

- Player

Goal:

- To choose a specific cipher type for learning and practice

Preconditions:

- Player has started the game
- Level selection interface is accessible

Postconditions:

- Selected cipher level is loaded
- Appropriate mode (Learn/Practice/Challenge) is made available based on progress

Main Flow:

1. System displays available cipher types
2. System shows progress status for each cipher
3. Player selects desired cipher level
4. System validates access requirements
5. System loads appropriate content and mode

Alternative Flow:

- If player selects a locked level, system displays prerequisite requirements
- If returning to a completed level, all modes are immediately accessible

Exceptions:

- If content loading fails, system returns to level selection with error message

3.3.3.2.3 Enter Learn Mode

Actors:

- Player

Goal:

- To access educational content and demonstrations for selected cipher

Preconditions:

- Player has selected a valid cipher level
- Learn Mode content is available for selected cipher

Postconditions:

- Historical content and demonstrations are loaded
- Interactive learning interface is displayed

Main Flow:

1. System loads historical content
2. System initializes interactive demonstrations
3. Player is presented with split-screen interface
4. System enables navigation through learning content

Alternative Flow:

- If player has previously completed this level, system offers quick review option

Exceptions:

- If content fails to load, system offers retry option or return to level selection

3.3.3.2.4 Enter Practice Mode

Actors:

- Player

Goal:

- To access practice exercises and cipher tools for hands-on learning

Preconditions:

- Player has completed Learn Mode for selected cipher
- Practice Mode is unlocked for selected level

Postconditions:

- Practice interface is displayed
- Cipher tools are available for use
- Practice exercises are loaded

Main Flow:

1. System initializes practice environment
2. System loads cipher tools
3. System presents available practice exercises
4. Player gains access to hint system
5. Exercise tracking system is activated

Alternative Flow:

- If returning to previous exercises, system loads saved progress
- System offers different difficulty levels based on performance

Exceptions:

- If tool initialization fails, system provides limited functionality mode

3.3.3.2.5 Enter Challenge Mode

Actors:

- Player

Goal:

- To attempt and solve cryptographic puzzles demonstrating mastery

Preconditions:

- Player has completed sufficient practice exercises
- Challenge Mode is unlocked for selected level

Postconditions:

- Challenge puzzle is loaded
- Required tools are accessible
- Solution submission system is activated

Main Flow:

1. System loads challenge puzzle
2. System initializes required cipher tools

3. System activates solution validation system
4. Player is presented with puzzle interface
5. Feedback system is enabled

Alternative Flow:

- If returning to previous challenge, system loads partial progress
- System offers alternate puzzles if stuck

Exceptions:

- If puzzle loading fails, system offers different puzzle or returns to level select

3.3.3.2.6 View Historical Content

Actors:

- Player

Goal:

- To learn historical context and theoretical background of selected cipher

Preconditions:

- Player is in Learn Mode
- Historical content is available for selected cipher

Postconditions:

- Player has accessed historical information
- System tracks content viewing progress

Main Flow:

1. System displays historical narrative and context
2. Player navigates through content sections
3. System highlights key concepts
4. Progress is automatically saved

Alternative Flow:

- If content was previously viewed, system offers quick review option

Exceptions:

- If content fails to load, system provides text-only fallback

3.3.3.2.7 Interact with Demonstration

Actors:

- Player

Goal:

- To understand cipher mechanics through interactive examples

Preconditions:

- Player is in Learn Mode
- Demonstration tools are initialized

Postconditions:

- Player has interacted with demonstration
- System records completion of demonstration

Main Flow:

1. System presents interactive cipher demonstration
2. Player follows guided steps
3. System provides real-time visualization
4. System validates player understanding through simple exercises

Alternative Flow:

- System provides additional examples if needed
- Player can replay demonstrations

Exceptions:

- If demonstration fails or unavailable, system provides static example

3.3.3.2.8 Use Cipher Tools

Actors:

- Player

Goal:

- To utilize encryption/decryption tools for solving puzzles

Preconditions:

- Player is in Practice or Challenge Mode
- Cipher tools are available for current level

Postconditions:

- Tool operations are performed

- Results are displayed to player

Main Flow:

1. Player selects desired cipher tool
2. System activates tool interface
3. Player inputs data for encryption/decryption
4. System processes input
5. System displays results

Alternative Flow:

- Tool provides intermediate steps for learning purposes
- System suggests appropriate tools based on context

Exceptions:

- If tool operation fails, system provides error message and recovery options

3.3.3.2.9 Attempt Exercise

Actors:

- Player

Goal:

- To complete practice exercises using learned concepts

Preconditions:

- Player is in Practice Mode
- Exercise content is loaded

Postconditions:

- Exercise attempt is recorded
- Feedback is provided to player

Main Flow:

1. System presents practice exercise
2. Player accesses necessary tools
3. Player works on solution
4. System validates attempt
5. System provides immediate feedback

Alternative Flow:

- System adjusts difficulty based on performance
- Additional practice exercises are provided if needed

Exceptions:

- If validation fails, system preserves progress and offers retry

3.3.3.2.10 Request Hints

Actors:

- Player

Goal:

- To receive guidance when stuck on exercises or challenges

Preconditions:

- Player is in Practice or Challenge Mode
- Hint system is available for current puzzle

Postconditions:

- Hint is displayed
- Hint usage is recorded

Main Flow:

1. Player activates hint system
2. System determines appropriate hint level
3. System displays contextual hint
4. Progress tracking is updated

Alternative Flow:

- Progressive hints are provided if needed
- System suggests reviewing specific concepts

Exceptions:

- If hint system unavailable, system provides basic guidance

3.3.3.2.11 Solve Puzzle

Actors:

- Player

Goal:

- To decrypt and solve challenge puzzles demonstrating mastery of cipher concepts

Preconditions:

- Player is in Challenge Mode
- Challenge puzzle is loaded
- Necessary tools are available

Postconditions:

- Puzzle attempt is tracked
- Progress toward solution is saved

Main Flow:

1. System presents encrypted puzzle message
2. Player analyses encryption pattern
3. Player uses cipher tools to work on solution
4. System tracks solution progress
5. Player prepares final solution

Alternative Flow:

- Player can save partial progress and return later
- System provides context clues based on progress

3.3.3.2.12 Submit Solution

Actors:

- Player

Goal:

- To verify puzzle solution and complete challenge

Preconditions:

- Player has attempted to solve puzzle
- Solution submission system is active

Postconditions:

- Solution is validated
- Challenge completion status is updated
- Progress is recorded

Main Flow:

1. Player submits proposed solution
2. System validates submission
3. System checks solution accuracy
4. System records attempt
5. System updates completion status

Alternative Flow:

- If solution is incorrect, system allows retry
- System provides targeted feedback on errors

3.3.3.2.13 Receive Feedback

Actors:

- Player

Goal:

- To receive detailed feedback on submitted solutions and overall performance

Preconditions:

- Player has submitted a solution
- Feedback system is operational

Postconditions:

- Feedback is displayed
- Learning recommendations are provided
- Performance metrics are updated

Main Flow:

1. System analyses submitted solution
2. System generates performance metrics
3. System provides specific feedback points
4. System offers improvement suggestions
5. Progress tracking is updated

Alternative Flow:

- System provides comparative performance data
- Additional practice recommendations are given if needed

Exceptions:

- If detailed feedback unavailable, system provides basic correct/incorrect response

3.3.3.2.14 View Progress

Actors:

- Player

Goal:

- To review completion status and performance across different ciphers

Preconditions:

- Player has accessed level selection
- Progress tracking system is functional

Postconditions:

- Progress information is displayed
- Achievement status is updated

Main Flow:

1. System retrieves progress data
2. System displays completion status for each cipher
3. System shows unlocked/locked content
4. System presents achievement progress

5. Performance statistics are displayed

Alternative Flow:

- System provides learning path recommendations
- Detailed statistics available on request

Exceptions:

- If progress data is corrupted, system displays last known valid state

3.4 Game Design

3.4.1 Core Game Loop

The core game loop of Crypto Chronica follows a "Learn-Practice-Challenge" structure designed to ensure effective learning through graduated exposure and application. Each level follows this three-phase progression to introduce and reinforce cryptographic concepts.

Figure 3.3: Gameplay Loop

In the Learn phase, players encounter new cryptographic concepts through a split-screen interface combining historical narrative with interactive demonstrations. The left panel presents historical context through story-driven content, while the right panel provides live demonstrations of encryption methods. This dual approach helps players understand both the historical significance and practical application of each cipher.

The Practice phase transitions to a workspace-focused interface where players can freely experiment with the encryption methods. This interface provides all necessary cryptographic tools and allows for unrestricted experimentation without the pressure of solving specific puzzles. Immediate feedback helps players understand the relationship between their actions and encryption outcomes.

The Challenge phase presents a focused interface combining the encrypted message, workspace, and necessary tools for solving actual cryptographic puzzles. This phase tests player understanding through practical application while maintaining access to relevant tools and hints.

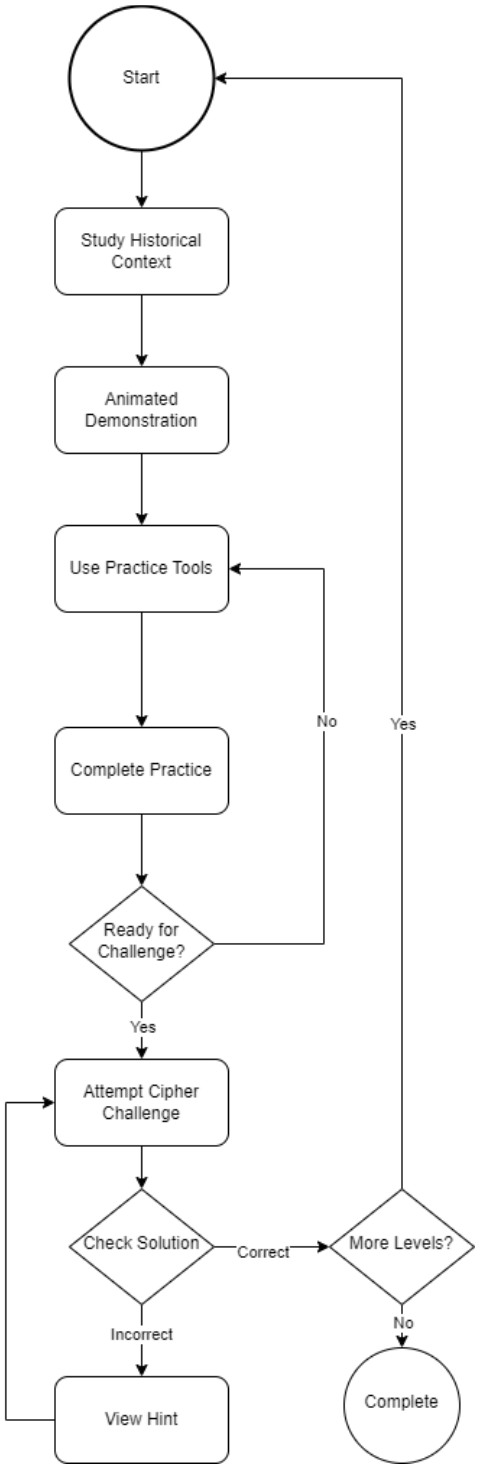


Figure 3.4: Activity Diagram - Level Progression on Learning

The detailed flow of player activities within each phase demonstrates the interactive nature of the learning process. In the Learn phase, players progress from historical context to hands-on demonstration, ensuring conceptual understanding before advancement. The Practice phase implements a feedback loop where players can experiment with tools and attempt example problems until they demonstrate sufficient understanding. The Challenge phase incorporates a hint system and solution validation, allowing players to attempt puzzles multiple times while receiving appropriate guidance.

3.4.2 Navigation Interface Layouts

The game's navigation system consists of two primary interfaces that guide players through the game. The main menu serves as the entry point to the game, providing essential options for starting or continuing the learning experience. The level selection screen then presents the available ciphers in a structured progression that reflects their historical development.

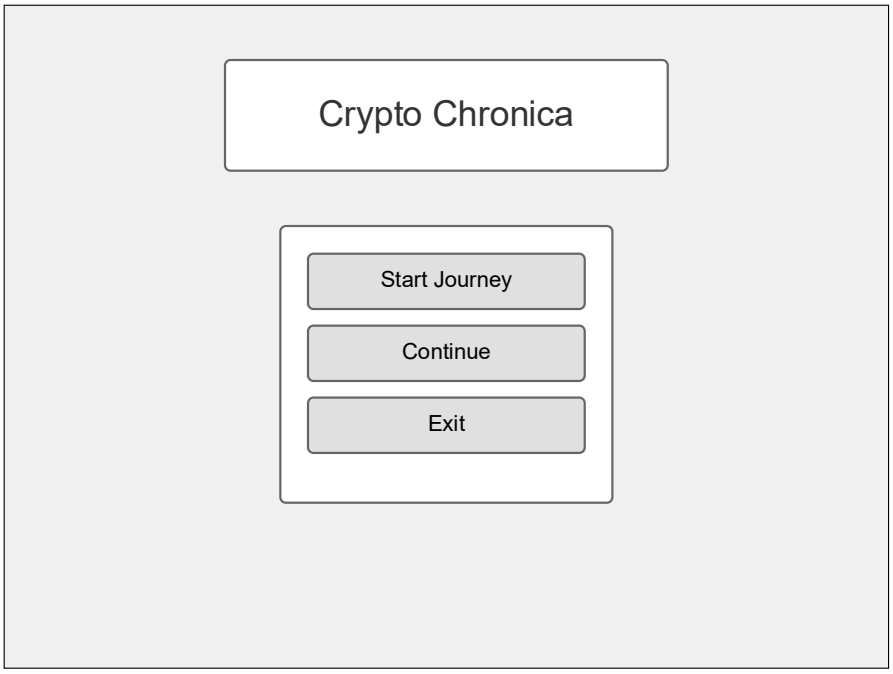


Figure 3.5: UI Layout for Main Menu

The main menu interface maintains a clean, focused design that emphasizes the core pathways through the game. Through this interface, players can initiate a new learning journey or resume their previous progress.

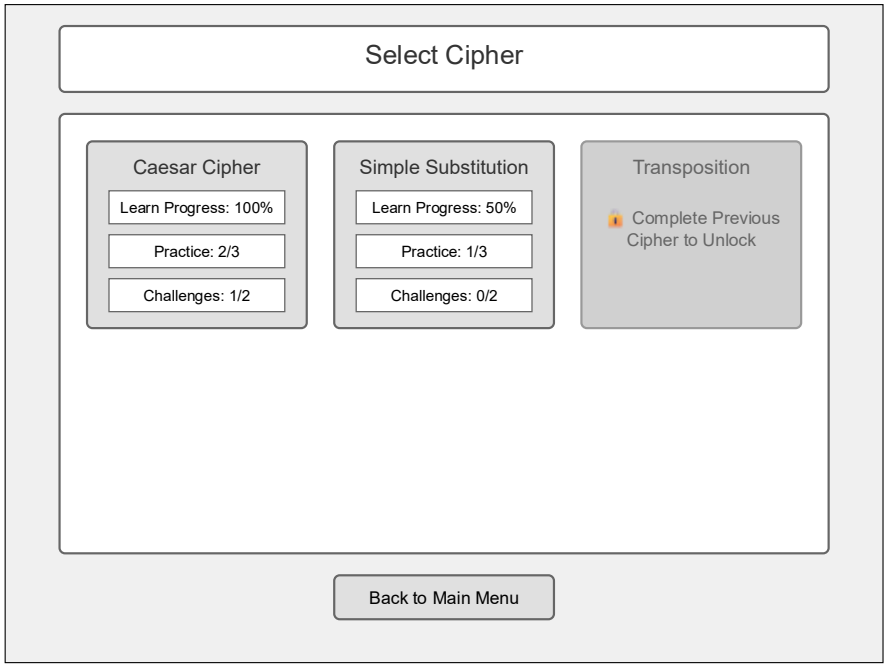


Figure 3.6: UI Layout for Level Select

The level selection interface presents cipher types in a progressive sequence, displaying individual progress metrics for each learning phase. Each cipher card shows completion status across Learn, Practice, and Challenge phases, helping players track their advancement. The interface implements a progression system where advanced ciphers become available as players demonstrate mastery of fundamental concepts, ensuring a structured learning experience.

3.4.3 Gameplay Interface Layouts

Each phase of the game requires distinct interface layouts and interactions:

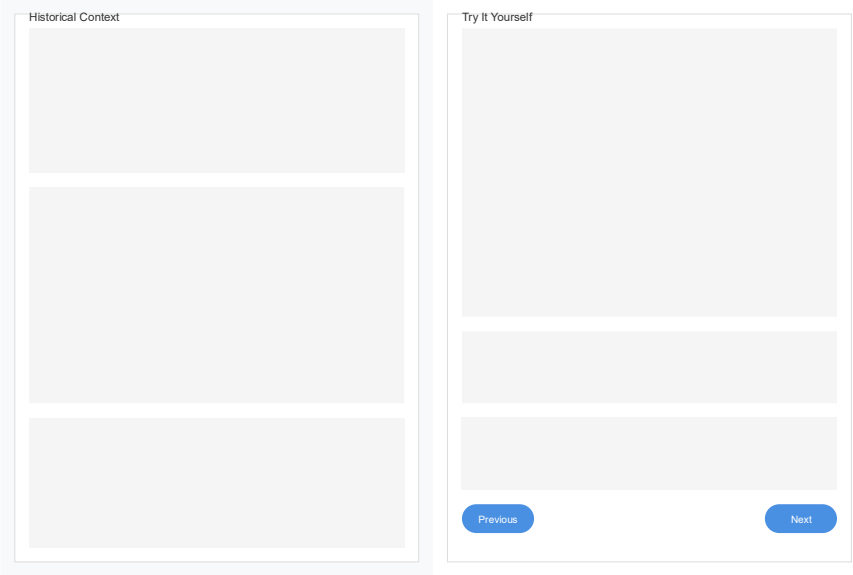


Figure 3.7: UI Layout for Learn Phase

The Learn phase interface emphasizes clear information presentation and basic interaction. Historical content is presented through text and visuals on the left, while interactive demonstrations on the right allow players to experiment with basic encryption concepts. Navigation controls allow smooth progression through the learning content.

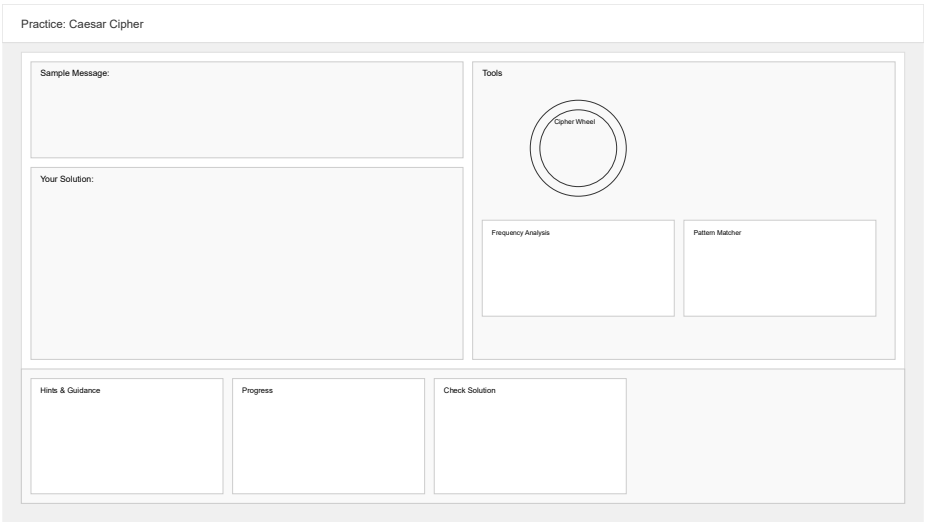


Figure 3.8: UI Layout for Practice Phase

The Practice phase interface introduces the complete set of cryptographic tools while maintaining a clean, uncluttered workspace. Tools include cipher wheel, frequency analysis, and pattern matching.

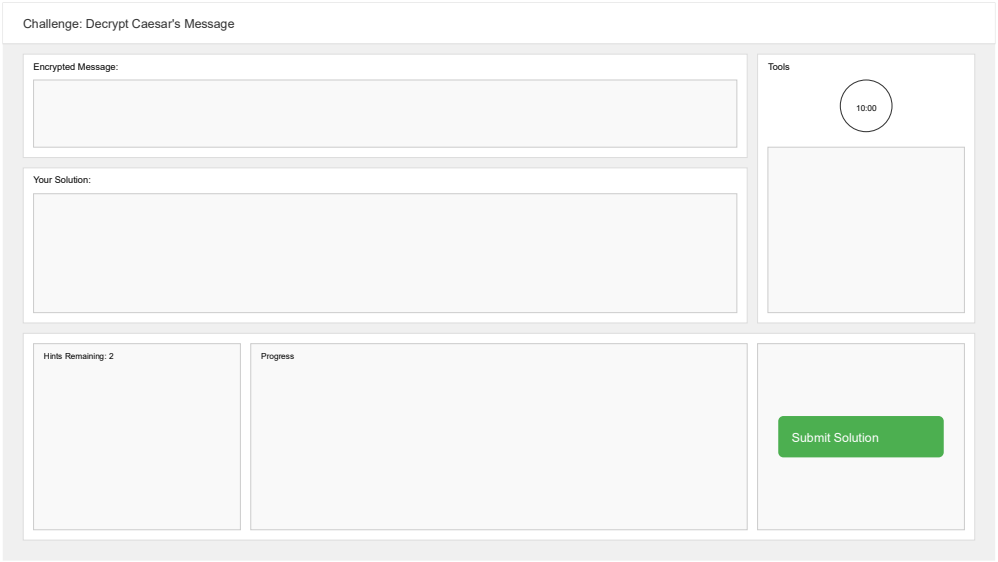


Figure 3.9: UI Layout for Challenge Phase

The Challenge phase combines all necessary elements for puzzle-solving while maintaining focus on the current task. The interface includes:

1. Encrypted message display
2. Working space for solution and tools
3. Relevant cryptographic tools
4. Hint system access
5. Progress tracking

3.4.4 Learning Progression System

The learning progression system in Crypto Chronica follows a structured approach that builds complexity gradually while ensuring fundamental concepts are mastered. Rather than relying on complex adaptive systems, the progression is designed around carefully crafted difficulty levels within each cipher type.

For each cipher, difficulty is managed through controllable elements:

1. Message length and complexity
2. Word selection (from common to rare)

3. Presence or absence of word spacing
4. Number of provided starting letters
5. Availability of contextual hints

The progression system tracks basic completion metrics:

1. Success in completing puzzles
2. Number of hints used
3. Time taken to solve

When players struggle with a particular concept, the system provides additional practice puzzles with simpler messages in the practice phase, review of related concepts from previous levels in the learn phase, and more detailed hints and guidance.

The level progression follows a historically grounded path through cryptographic methods, from simple substitution ciphers to more complex methods. Each new cipher type builds upon knowledge gained from previous levels, ensuring players have the necessary foundation before advancing. For instance:

1. Caesar Cipher introduces basic letter substitution
2. Simple substitution expands on letter replacement concepts
3. Pattern recognition builds on substitution knowledge

This structured approach maintains educational integrity while providing appropriate support for different learning rates. The system focuses on ensuring thorough understanding of each concept rather than rushing progression, allowing players to build confidence through practice before tackling more complex challenges.

3.5 Implementation Plan

3.5.1 Development Phases

The development of Crypto Chronica follows a phased approach that builds complexity gradually following the iterative development methodology. Each phase focuses on specific aspects of the game while allowing for continuous refinement based on testing and evaluation.

Phase 1 establishes the core framework, focusing on fundamental game mechanics and basic cryptographic implementation. This phase prioritizes creating a stable foundation upon which subsequent features can be built. The primary focus includes implementing the basic user interface structures for all three main phases (Learn, Practice, and Challenge), developing the navigation system between game phases, and creating the data persistence foundation. The Caesar cipher serves as the initial cryptographic implementation, complete with an interactive cipher wheel tool and basic tutorial system.

Phase 2 expands the educational content and core features of the game. This phase focuses on integrating historical content, implementing the learning progression system, and developing the achievement tracking system. Additional cipher implementations including simple substitution and related tools like pattern recognition and frequency analysis are introduced. The phase emphasizes refinement of educational content effectiveness and smooth progression between concepts.

Phase 3 focuses on system refinement and core feature completion. During this phase, the emphasis shifts to performance optimization, user interface polish, and expanding the content with additional practice puzzles. The hint system receives comprehensive implementation, progress tracking is refined, and the achievement system is completed. This phase ensures system stability and overall learning effectiveness.

Phase 4 outlines future enhancements and advanced content implementation. The centrepiece of this phase would be the implementation of the Enigma machine simulation, which serves as an advanced challenge that combines concepts from previous ciphers. The Enigma implementation would require players to understand substitution, pattern recognition, and mechanical encryption principles, creating a culminating experience that tests mastery of the game's core concepts. Additional enhancements in this phase could include expanded practice exercises, advanced puzzle variations, and optimization of existing features.

Each development phase includes iterative cycles of implementation, testing, and refinement, ensuring that features are thoroughly validated before moving forward. This approach allows for continuous improvement while maintaining consistent development progress.

3.5.2 Testing Strategy

The testing strategy for Crypto Chronica emphasizes systematic validation of both technical functionality and educational effectiveness through self-directed testing approaches. This strategy ensures thorough verification of features while maintaining development efficiency.

Development testing forms the core of the validation process, focusing on three key areas. Component testing verifies individual features such as cipher implementations, interface functionality, and data management systems. Educational testing evaluates the effectiveness of tutorials, validates learning progression, and assesses the difficulty curve of puzzles and challenges. System testing examines feature integration, overall performance, and the cohesiveness of the user experience.

The testing process is a main part of the iterative development cycle, allowing for continuous improvement based on findings. Each implemented feature undergoes initial validation followed by integration testing to ensure compatibility with existing components. This

approach helps identify and address issues early in the development process while maintaining steady progress toward project goals.

3.6 Summary

Chapter 3 has outlined the comprehensive design and development approach for Crypto Chronica, establishing the foundation for an educational game that teaches cryptography through interactive puzzles. The chapter detailed the iterative development methodology that will guide the project's implementation, ensuring systematic progress through well-defined development cycles.

The requirements analysis established both functional and non-functional requirements, providing a clear framework of essential features needed for an effective educational game. Through detailed use cases, key interactions and workflows are mapped out that form the backbone of the game's functionality.

The game design section introduced the core Learn-Practice-Challenge structure, detailing how this progression supports the learning process while maintaining engagement. Interface designs for each phase were carefully specified to support both educational objectives and user interaction needs, with clear layouts that facilitate learning and gameplay.

The implementation plan provided a clear roadmap through three development phases, along with testing strategies to ensure both technical functionality and educational effectiveness. This systematic approach to development and testing will help maintain focus on core functionalities while allowing for iterative improvements.

This comprehensive planning and design framework provides the blueprint for developing Crypto Chronica as an engaging and effective educational tool for teaching cryptography concepts. The clear definition of requirements, game design elements, and implementation strategy sets a strong foundation for the development phase of the project.

Chapter 4: Implementation

4.1 Implementation Overview

The implementation of Crypto Chronica translates the educational game design into a functional cryptography learning tool using the Godot 4.4 game engine. The system implements a three-phase learning progression (Learn-Practice-Challenge) through modular scene architecture, with mathematical cipher implementations maintaining cryptographic accuracy while providing engaging user interfaces.

4.1.1 Technology Stack and Architecture

The application uses Godot's node-based architecture with GDScript for core logic implementation. Each learning phase exists as an independent scene, enabling dynamic loading based on user progression. The GameProgressManager autoload singleton provides centralized state management and persistence across all educational phases.

Core cryptographic algorithms are implemented as standalone classes (CaesarCipher, SubstitutionCipher) that operate independently of the user interface, ensuring mathematical accuracy and enabling future expansion. Educational content is externalized through JSON data structures, separating content from code for rapid iteration.

The modular design supports the iterative development methodology, with each cipher type and learning phase functioning as discrete components that integrate through standardized interfaces. This architecture enables systematic testing and validation while maintaining educational progression integrity.

4.2 Development Environment and Tools

The development of Crypto Chronica utilizes Godot 4.4 as the primary development platform, selected for its scene-based architecture that naturally supports the modular educational content structure required for the three-phase learning system. The engine's node hierarchy provides the necessary abstraction between cryptographic algorithms and user interface presentation, enabling complex educational interactions without exposing computational complexity to learners.

The project architecture implements a clear separation between cryptographic logic and educational presentation through standalone cipher classes that maintain mathematical accuracy independently of the game engine. The codebase organization follows a hierarchical structure where global systems exist as singleton autoload objects, while scene-specific controllers manage local educational interactions within each learning phase.

Educational content management is achieved through JSON-based data structures that externalize historical narratives, exercise definitions, and challenge scenarios from the technical implementation. This separation enables rapid content iteration without requiring code modifications, directly supporting the iterative development methodology while maintaining system stability during educational content refinement.

Version control implementation follows a linear development model where the main branch consistently maintains a functional educational experience suitable for testing and validation. The development workflow emphasizes educational verification alongside technical implementation, with each cipher algorithm validated against examples and specifications before integration into the framework.

4.3 Core Game Systems Implementation

The core game systems provide the foundational infrastructure for educational content delivery and user progression tracking through centralized state management and consistent navigation interfaces.

4.3.1 Game Progress Management System

The GameProgressManager implements persistent learning state tracking through an autoload singleton that maintains completion status across all cipher types and learning phases. The system utilizes a hierarchical data structure that captures granular progress information including exercise completion, hint usage statistics, completion times, and performance metrics for comprehensive educational assessment.

The progressive unlocking system automatically manages phase transitions and cipher availability based on completion criteria, implementing the educational prerequisite structure where advanced concepts become accessible only after demonstrating mastery of fundamental principles. Challenge set progress tracking incorporates a specialized timer system that accurately measures time-on-task across multiple sessions while accounting for pause states during navigation interruptions.

4.3.2 Navigation and State Management

The navigation framework implements seamless transitions between educational phases while preserving learning context and progress status. The level selection interface provides visual progress representation where each cipher displays completion indicators across all three learning phases, enabling learners to understand their position within the overall curriculum.

Figure 4.1: Level Select Menu

The figure above shows the level select screen where the progress of the user in completing the phases of a cipher can be viewed. Scene transition management implements state preservation that maintains educational context across navigation events, ensuring that learners can resume educational activities after interruptions without losing current work or progress status. The system handles complex state scenarios including in-progress challenge solutions, cipher tool configurations, and partially completed exercises through centralized state management that provides consistency across all learning phases.

The persistence mechanism utilizes JSON serialization to maintain human-readable save files that preserve educational progress across application sessions. The save system implements automatic progress preservation at key educational milestones while minimizing system overhead during active learning sessions.

4.4 Learning Progression System Implementation

4.4.1 Three-Phase Learning Structure

The Learn Phase implements historical content presentation through a dual-panel interface combining narrative text with interactive demonstrations. The system loads educational content from JSON data structures that separate historical narratives from presentation logic, enabling content modification without code changes. Interactive demonstrations are embedded as cipher tool instances that respond to user manipulation while providing contextual explanations of cryptographic transformations.

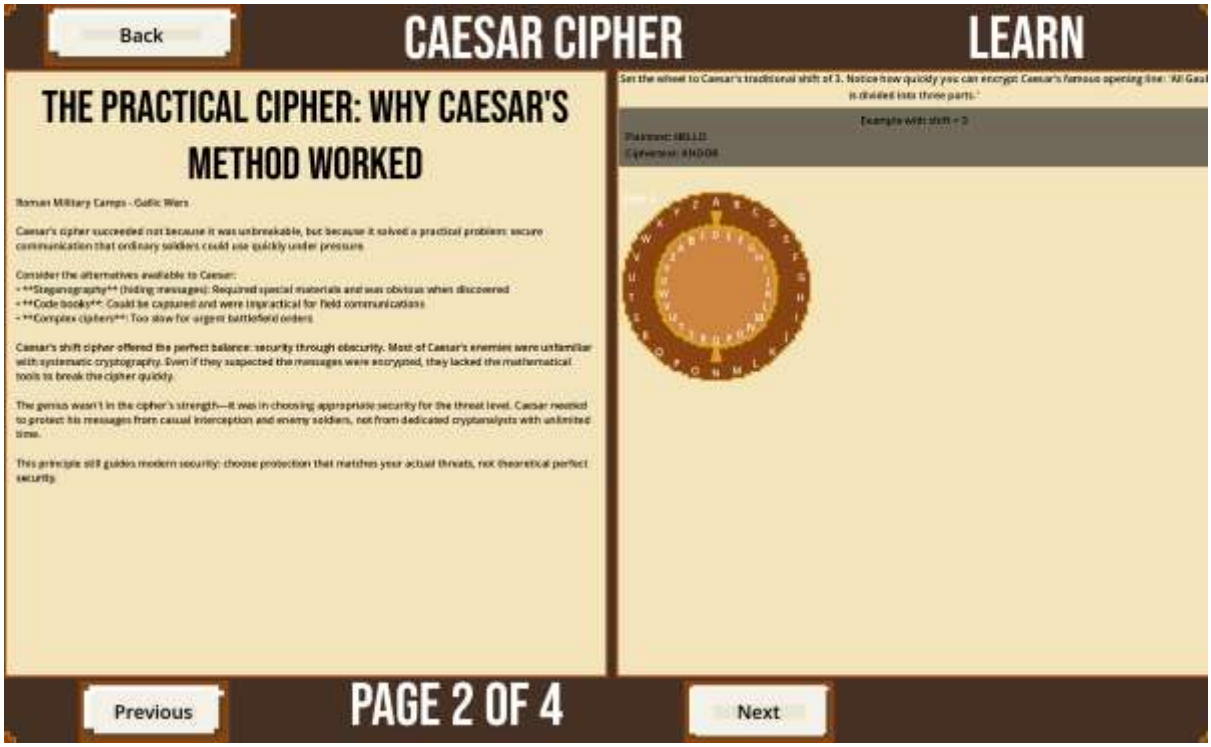


Figure 4.2: Learn Phase

The figure above shows the Caesar Cipher Learn Phase on the second page of four with the caesar wheel on the right panel. The Learn Phase implementation presents historical content through a dual-panel interface that combines narrative text with interactive demonstrations. The system loads historical data from JSON files that separate content from presentation logic, enabling rapid iteration on educational narratives while maintaining technical stability.

Interactive demonstrations are implemented as embedded cipher tools that respond to user manipulation while providing contextual explanations of cryptographic transformations.

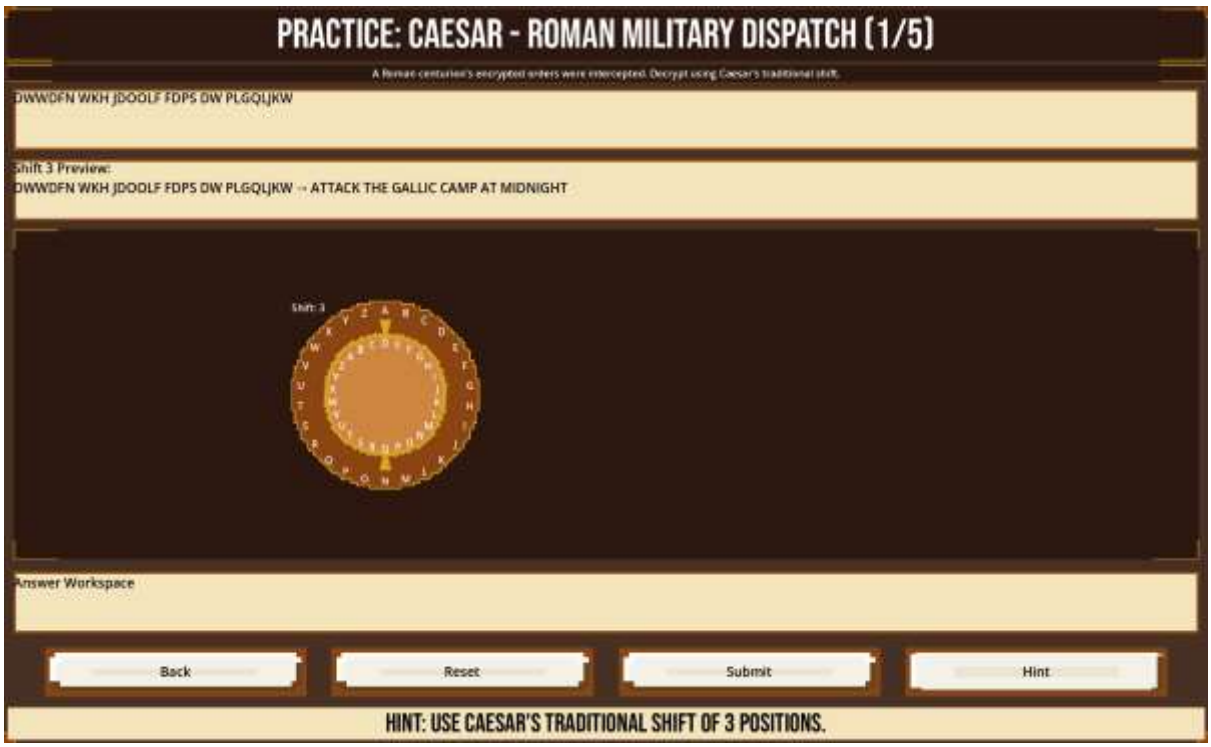


Figure 4.3: Practice Phase

The Practice Phase implementation transitions learners to active cipher manipulation through structured exercises that build understanding through hands-on application. The system implements exercise validation that provides immediate feedback on correctness while offering contextual hints that guide learners toward correct solutions. The phase has 2 types of tasks which are to encrypt or to decrypt.

Figure 4.4: Challenge Hub

The Challenge Phase implementation presents cryptographic puzzles that require synthesis of concepts learned in previous phases. The user begins the challenge phase by choosing their preferred challenge set as shown in figure 4.4. The system implements a card-based challenge structure where each card is an individual puzzle, with those answers providing an answer for the main question in the challenge set. Challenge validation includes sophisticated answer checking that accepts multiple correct formats while providing fixed feedback on partial solutions.

4.4.2 Content Management and Delivery System

The content management system implements a structured approach to educational material organization that separates historical narratives, exercise definitions, and challenge scenarios into discrete, manageable components. This separation enables independent development and testing of educational content while maintaining technical system stability.

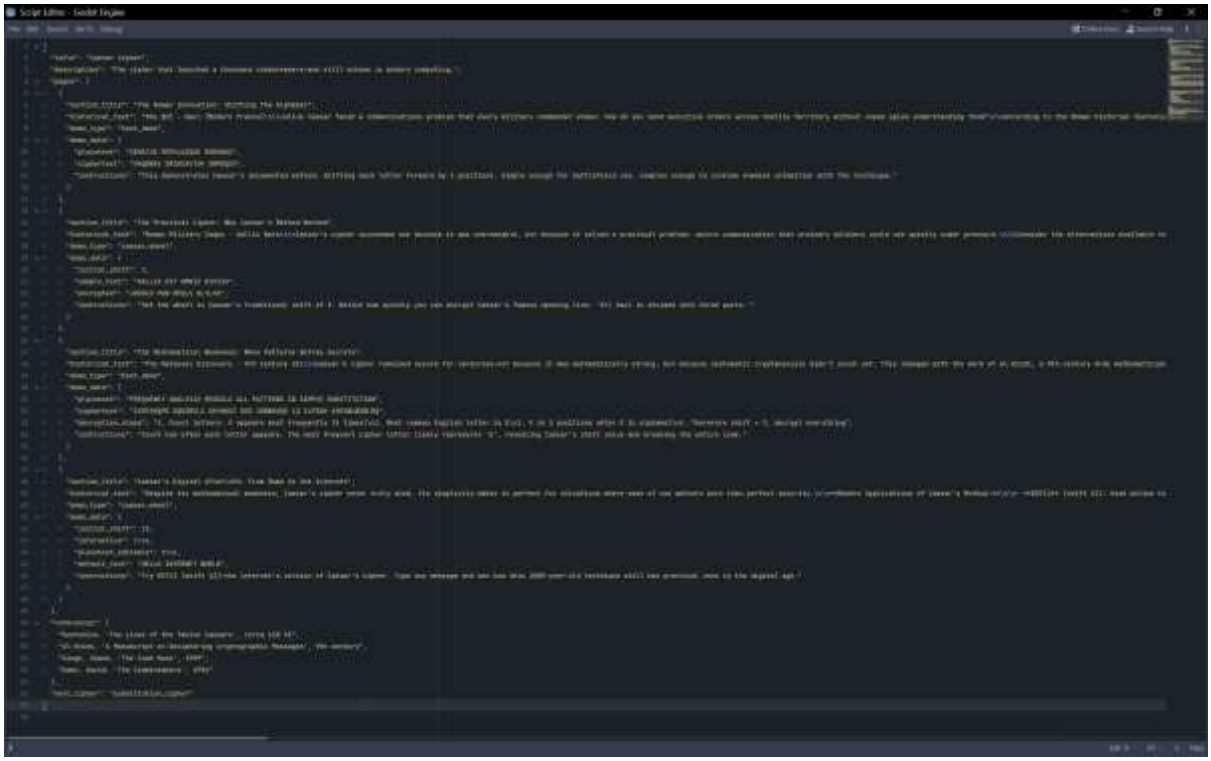


Figure 4.5: Code implementation of JSON file

Figure 4.5 above shows an example of the way the data is stored in a JSON file which allow for quick iterations of content.

Historical content for the Learn Phase is structured through JSON files that define page sequences, demonstration types, and interactive elements. The system supports multiple demonstration formats including static text examples, interactive cipher wheels, and substitution table manipulations. Content loading is implemented dynamically, enabling the system to present appropriate demonstrations based on the specific cipher being studied and the learner's current progress level.

Exercise content implements a flexible definition system that supports multiple task types which are encryption and decryption. Exercise definitions include expected solutions, hint sequences, and task parameters that enable the system to provide appropriate guidance and assessment. The validation system implements answer checking that accounts for formatting variations while maintaining cryptographic accuracy requirements.

Challenge content implements a narrative-driven structure where individual cipher puzzles are embedded within historical scenarios that provide context and motivation for problem-solving activities. Challenge sets include progression dependencies, timing requirements, and performance metrics that support both immediate learner feedback and comprehensive educational assessment.

4.4.3 Assessment and Feedback Integration

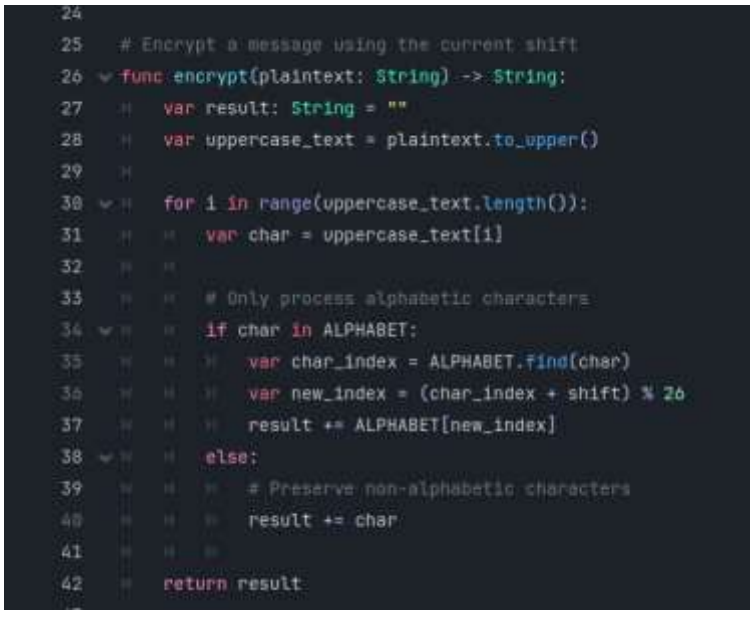
The learning progression system implements continuous assessment mechanisms that provide immediate feedback on learner actions while maintaining progress tracking for educational evaluation purposes. Immediate feedback systems provide real-time responses to learner interactions with cipher tools, displaying encryption results, highlighting correct mappings, and indicating progress toward solution goals. The feedback implementation uses visual highlighting, audio cues, and textual confirmations to reinforce correct understanding while gently redirecting incorrect approaches without discouraging continued engagement.

4.5 Cryptographic Tools Implementation

4.5.1 Caesar Cipher Implementation

The Caesar cipher implementation provides the mathematical foundation for all Caesar cipher operations within the educational framework while maintaining historical accuracy and computational efficiency. The implementation is structured as an independent class that encapsulates encryption, decryption, and key management operations without dependencies on the user interface system.

The core algorithm implements the mathematical transformation for Caesar cipher operations using modular arithmetic to ensure correct handling of alphabet wraparound. The implementation maintains the traditional 26-letter English alphabet constraint while providing robust error handling for edge cases and invalid input parameters.



```
24
25  # Encrypt a message using the current shift
26  func encrypt(plaintext: String) -> String:
27      var result: String = ""
28      var uppercase_text = plaintext.to_upper()
29
30      for i in range(uppercase_text.length()):
31          var char = uppercase_text[i]
32
33          # Only process alphabetic characters
34          if char in ALPHABET:
35              var char_index = ALPHABET.find(char)
36              var new_index = (char_index + shift) % 26
37              result += ALPHABET[new_index]
38          else:
39              # Preserve non-alphabetic characters
40              result += char
41
42      return result
```

Figure 4.6: Code implementation of encrypt function caesar cipher

Figure 4.6 shows one of the functions within the caesar cipher implementation which is the encrypt function. The shift management system implements validation mechanisms that ensure shift values remain within valid ranges while supporting both positive and negative shift operations. The implementation handles shift values outside the 0-25 range through modular

arithmetic, ensuring mathematical correctness regardless of input parameters while maintaining educational clarity about the underlying transformations.

The class provides functionality for educational applications including brute force analysis capabilities that generate all possible decryption outcomes for cipher breaking exercises. This functionality supports the Challenge phase requirements where learners must analyze multiple potential solutions to identify correct decryptions based on language patterns and contextual clues.

4.5.2 Interactive Cipher Wheel Component

The cipher wheel implementation creates an interactive visualization of the Caesar cipher that bridges the conceptual gap between mathematical operations and the historical physical tools used for encryption. The component implements drag-based rotation mechanics that provide intuitive manipulation while maintaining precise control over shift values.

The visual design implements a dual-ring structure where the outer ring displays the standard alphabet while the inner ring rotates to show the cipher alphabet corresponding to the current shift value. The implementation ensures that letter alignments remain precise during rotation while providing clear visual indication of the encryption mapping for any given shift value. The wheel is as follows in Figure 4.7.

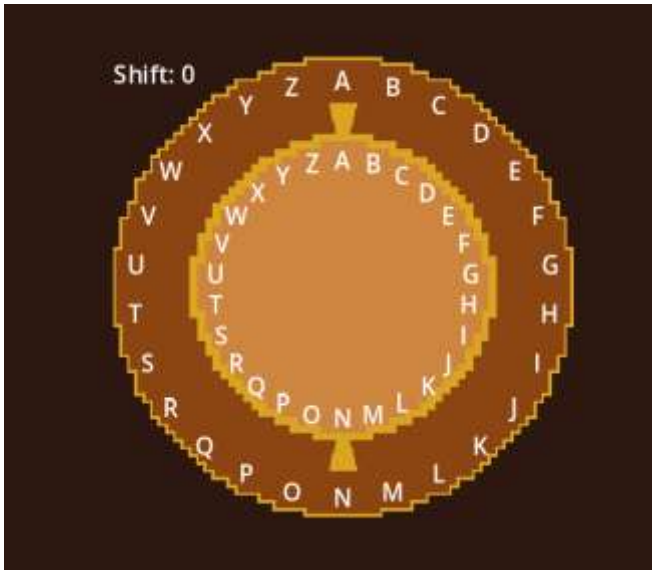


Figure 4.7: Caesar Cipher Wheel

The rotation mechanics implement smooth animation and snapping behavior that provides satisfying tactile feedback while ensuring that the wheel settles on precise shift values. The system provides audio feedback during manipulation that reinforces the discrete nature of cipher shifts while avoiding excessive audio distraction during extended use.

4.5.3 Substitution Cipher Implementation

The substitution cipher implementation provides support for arbitrary letter-to-letter mapping while maintaining the mathematical rigor required for educational cryptography applications. The system implements full key validation, frequency analysis capabilities, and multiple key generation methods that support various educational scenarios from guided learning to independent problem-solving.

The core substitution algorithm implements bijective letter mapping with validation to ensure that cipher keys maintain the one-to-one correspondence required for reversible encryption. The implementation detects and prevents duplicate mappings while providing clear error feedback when invalid keys are attempted.

Key generation capabilities include random key generation, keyword-based key derivation, and Atbash cipher implementation. These methods provide educational variety while demonstrating different approaches to substitution key creation that have been used historically. The keyword-based generation implements the historical method of using memorable phrases to create cipher keys while removing duplicate letters and completing the alphabet systematically.

Frequency analysis functionality implements letter counting and statistical analysis that supports the Challenge phase requirements for cipher breaking activities. The system calculates letter frequencies, identifies common patterns, and provides suggestions for likely letter mappings based on English language characteristics. This capability enables learners to experience authentic cryptanalysis techniques while working with appropriately sized message samples.

4.5.4 Interactive Substitution Table Component

The substitution table implementation provides an interface for constructing and manipulating substitution cipher keys through direct manipulation of letter mappings. The component implements drag-and-drop functionality that enables learners to build cipher keys intuitively while maintaining the mathematical constraints required for valid substitution ciphers. Figure 4.8 shows the substitution table used to assign the plain letters to its cipher letters counterpart.

Figure 4.8: Substitution table

The visual design implements a two-row table structure where plaintext letters are displayed in alphabetical order with corresponding cipher letters positioned directly below. The interface provides immediate visual feedback for mapping completeness and validity while highlighting potential conflicts or missing assignments that would prevent successful encryption or decryption operations.

The drag-and-drop system addresses the fundamental challenge of making substitution cipher manipulation feel engaging rather than purely functional. While the underlying one-to-one letter mapping is mathematically straightforward, translating this into an interface that maintains game-like qualities required careful consideration of user interaction patterns. The implementation provides intelligent conflict resolution that automatically swaps letters when conflicts arise, preventing the creation of invalid cipher keys while maintaining the tactile satisfaction of direct manipulation.

This design approach represents a compromise between mathematical precision and interface engagement. Unlike the Caesar wheel, which naturally maps to the physical metaphor of rotation, substitution ciphers have no obvious physical analog, making interface design more difficult. The table structure ensures clarity and educational transparency, while the drag-and-drop mechanics add game-like elements that set the experience apart from standard digital worksheets.

4.5.5 Pattern Analysis Tool Integration

The pattern analysis implementation provides sophisticated frequency analysis and pattern recognition capabilities that support the educational objectives for substitution cipher cryptanalysis. The tool implements multiple analysis modes including frequency analysis, pattern matching, and word-based analysis that accommodate different message characteristics and learning approaches.

Frequency analysis implements letter counting with visual representation through bar charts and statistical displays. The system calculates both raw frequencies and percentage distributions while providing comparison with expected English language frequencies. This comparison enables learners to identify likely letter correspondences based on statistical analysis of cipher text samples.

Pattern recognition capabilities include identification of repeated letter sequences, single-letter words, and common word patterns that can provide cryptanalytic insights even with limited frequency data. The system highlights these patterns within cipher text while providing suggestions for likely plaintext correspondences based on English language characteristics. Figure 4.9 shows the cryptanalysis tool with an analysis on a cipher text and its top suggestions.

Figure 4.9: Cryptanalysis Tool

Integration with the substitution table component enables learners to apply analysis results directly to cipher key construction. The system provides suggestion mechanisms that can automatically populate table entries based on analysis results while maintaining user control over the cryptanalysis process. This integration supports the hands-on learning approach where learners actively construct solutions based on their analysis rather than passively receiving answers.

4.6 Challenge System Implementation

4.6.1 Challenge Set Architecture

The challenge system implements a narrative-driven puzzle framework that presents cryptographic problems within historical contexts, providing learners with authentic scenarios that demonstrate the practical applications and limitations of classical cipher systems. The architecture separates challenge content from presentation logic through JSON-based data structures that enable rapid development of new scenarios while maintaining consistent educational objectives and assessment criteria.

Each challenge set implements a multi-card structure where individual puzzles build toward a master question that requires synthesis of information gathered from component challenges. This approach mirrors authentic cryptanalytic scenarios where intelligence analysts must piece together information from multiple sources to understand complete communications or identify security threats.

The card-based structure provides modular challenge components that can be approached individually while contributing to the overall narrative and educational objectives. Each card presents a specific cryptographic puzzle with contextual information that enhances the historical authenticity and provides motivation for problem-solving activities.

Challenge validation implements sophisticated answer checking that accommodates multiple correct formats while maintaining cryptographic accuracy requirements. The system recognizes variations in capitalization, spacing, and word ordering for answers that may have multiple valid expressions, while ensuring that the underlying cryptographic analysis demonstrates correct understanding of cipher principles.

4.6.2 Challenge Hub and Set Selection

The challenge hub implements a centralized interface for accessing multiple challenge sets within each cipher type, providing learners with variety in cryptographic scenarios while maintaining educational consistency. The hub displays available challenge sets with progress indicators, difficulty ratings, and estimated completion times that help learners select appropriate challenges based on their current skill level and available time.

Challenge set cards display comprehensive information including narrative themes, difficulty levels, and progress status that enable informed selection decisions. The interface provides clear visual distinction between completed, partially completed, and untouched challenge sets, supporting learner autonomy in choosing educational activities while maintaining progress visibility.

The selection interface implements reset functionality that enables learners to restart challenge sets for practice purposes or to improve completion times. This functionality supports repeated engagement with challenging material while maintaining progress tracking for educational assessment purposes.

4.6.3 Timer Implementation and Time Tracking

The timing system implements accurate measurement of learner engagement with challenge content through timer management that accounts for pause states, navigation interruptions, and multi-session challenge completion. The implementation provides completion time measurement without influencing challenge difficulty or assessment criteria, serving purely as an informational metric for learner feedback.

Timer initialization and management occurs automatically when learners begin challenge sets, with pause functionality that activates during navigation away from challenge content or application interruptions. The system resumes timing automatically when learners return to active challenge engagement, ensuring accurate measurement of actual session duration across multiple learning periods.

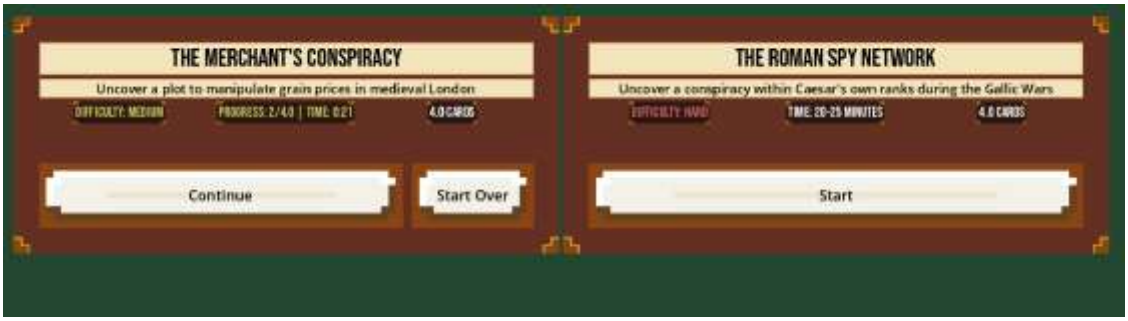


Figure 4.10: Challenge Sets with progress saved and displayed

The timing system maintains accumulated time across multiple sessions, enabling learners to work on challenging problems over extended periods without losing timing accuracy. The time is then displayed on the challenge set as seen on figure 4.10. This approach supports realistic learning patterns where complex cryptographic analysis may require multiple sessions or extended problem-solving periods.

Completion time display provides learners with feedback on their problem-solving duration upon challenge set completion. This information serves as personal progress indication without comparative or competitive elements, supporting intrinsic motivation for continued learning engagement.

4.6.4 Hint System Implementation

The hint system implements a fixed support structure that provides predetermined levels of assistance for each challenge card. The system delivers contextual guidance through a sequence

of hints that build progressively from general problem-solving approaches to more specific analytical directions.

Hint content is embedded within challenge card definitions, ensuring that guidance remains consistent and educationally appropriate for each specific cryptographic problem. The implementation provides three levels of hint support for most challenges, progressing from conceptual guidance through methodological suggestions to specific analytical approaches. The hint is displayed at the bottom of the interface as follows:

Figure 4.11: Hint system in action

The hint delivery system maintains simplicity in presentation while ensuring that learners can access appropriate levels of support when needed. Hint usage is tracked for informational purposes but does not influence challenge assessment or progression requirements, maintaining the educational focus on problem-solving process rather than solution efficiency.

Hint exhaustion handling provides clear feedback when all available hints have been accessed, encouraging learners to apply the provided guidance toward independent solution development.

4.6.5 Answer Validation and Feedback Systems

The answer validation system implements checking mechanisms that accommodate the complexity of cryptographic problem-solving while maintaining strict accuracy requirements for educational assessment. The system recognizes multiple valid answer formats while

ensuring that underlying cryptographic analysis demonstrates correct understanding of cipher principles.

Validation algorithms implement flexible string matching that accounts for variations in capitalization, spacing, and punctuation while maintaining semantic accuracy for cryptographic answers. The system distinguishes between formatting variations and conceptual errors, providing appropriate feedback that guides learners toward correct presentation without penalizing minor technical details. The implementation is as follows:

```
func _is_answer_correct(submitted: String, valid_answers: Array) -> bool:
    """Check if submitted answer matches any of the valid answers"""
    for valid_answer in valid_answers:
        if submitted == valid_answer:
            return true

        # Optional: Check for partial word matches
        if _check_word_match(submitted, valid_answer):
            return true

    return false
```

Figure 4.12: Answer validation code implementation

Error handling provides clear feedback for incorrect solutions while maintaining encouraging tone that supports continued problem-solving efforts. The system provides generic error messages that indicate incorrect solutions without revealing specific information that might compromise the educational value of independent analysis.

The feedback delivery system implements immediate response mechanisms that provide learners with clear indication of solution accuracy. Successful completion triggers positive feedback and enables progression to subsequent challenges, while incorrect attempts encourage continued analysis through supportive messaging that maintains learner engagement with challenging cryptographic problems.

4.7 Audio and User Experience Implementation

4.7.1 Audio Feedback System

The audio implementation provides contextual feedback to improve the educational experience without overpowering or distracting from the primary learning objectives. The system implements a audio manager that coordinates sound effects across all educational phases.

The audio architecture implements a polyphonic sound system that enables multiple audio events to occur simultaneously without interference, particularly important during cipher manipulation activities where users may perform rapid sequences of operations that require individual audio confirmation. The system manages audio channels dynamically to prevent audio buildup while ensuring that important feedback sounds remain audible. The implementation is as follows:

```
func play_ui_sound_polyphonic(sound_key: String, volume_modifier: float = 1.0) -> void:
    """Play UI sound with support for overlapping instances"""
    if not is_sfx_enabled:
        return

    var sound_path = ""
    if ui_sounds.has(sound_key):
        sound_path = ui_sounds[sound_key]
    elif cipher_interaction_sounds.has(sound_key):
        sound_path = cipher_interaction_sounds[sound_key]
    else:
        print("Unknown UI sound: ", sound_key)
        return

    var audio_stream = load(sound_path)
    if audio_stream:
        var player = _get_next_ui_player()
        player.stream = audio_stream
        player.volume_db = linear_to_db(volume_modifier)
        player.play()
```

Figure 4.13: Code implementation of polyphonic sound

Cipher-specific audio feedback provides distinct sound signatures for different types of cryptographic operations, helping learners develop auditory associations with specific cipher manipulations.

The audio system implements contextual awareness that adjusts sound selection based on the current educational phase and specific learning activities. Learn phase audio emphasizes gentle

confirmation sounds that support exploration without pressure, while Challenge phase audio provides more definitive feedback that clearly indicates success or failure in problem-solving attempts.

4.7.2 Scene-Specific Audio Management

Audio continuity across different educational phases is maintained through a scene-aware management system that transitions background audio smoothly while preserving the educational atmosphere. Each major educational phase implements distinct audio themes that reinforce the learning context while maintaining consistency with the overall educational experience. The game makes use of the plugin created by Ovani Sound to handle music playing and intensity of scene music. The implementation for scene music is as follows:

```
func set_audio_for_scene(scene_name: String) -> void:
    """Set both music and any scene-specific audio configuration"""
    match scene_name:
        "main_menu":
            play_music_for_scene("main_menu")
            set_music_intensity(0.5, 1.0)
        "level_select":
            play_music_for_scene("main_menu")
            set_music_intensity(0.3, 1.0)
        "learn_phase":
            play_music_for_scene("learn_phase")
            set_music_intensity(0.2, 1.5)  # Calm, focused
        "practice_phase":
            play_music_for_scene("practice_phase")
            set_music_intensity(0.4, 1.5)  # Moderate energy
        "challenge_hub":
            play_music_for_scene("challenge_hub")
            set_music_intensity(0.6, 1.0)  # Building tension
        "challenge_set":
            play_music_for_scene("challenge_set")
            set_music_intensity(0.7, 1.0)  # High tension
        "challenge_card_solver":
            # Keep current music but reduce intensity for focus
            set_music_intensity(0.3, 0.5)
        "completion":
            play_music_for_scene("completion", 0.5)  # Quick transition
            set_music_intensity(1.0, 0.5)  # Full triumphant
```

Figure 4.14: Code implementation of scene audio functionality

4.8 Summary

This chapter has detailed the technical implementation of Crypto Chronica, demonstrating the translation of educational game design specifications into a functional cryptography learning system. The implementation successfully realizes the three-phase learning progression through modular scene architecture built on the Godot 4.4 engine, with GDScript providing the computational foundation for mathematically accurate cipher implementations.

The core system architecture centers on the GameProgressManager singleton that maintains persistent educational state across all learning phases while supporting complex progression tracking including individual exercise completion, challenge set timing, and performance metrics collection. The navigation framework provides seamless transitions between educational contexts while preserving learning continuity through comprehensive state management and JSON-based progress persistence.

Cryptographic tool implementations achieve the critical balance between mathematical accuracy and engaging interaction through specialized interface components. The Caesar cipher wheel successfully translates abstract modular arithmetic into intuitive rotation mechanics, while the substitution table addresses the more complex challenge of making arbitrary letter mappings feel naturally manipulable through intelligent drag-and-drop conflict resolution.

The challenge system implements sophisticated narrative-driven puzzle delivery through card-based progression structures that require concept synthesis across multiple cryptographic problems. Integration of timer management, hint delivery, and flexible answer validation provides comprehensive assessment capabilities while maintaining educational rigor in cryptographic analysis requirements.

Audio system integration enhances the learning experience through contextual feedback mechanisms that support rather than interfere with primary educational objectives. The polyphonic audio architecture ensures responsive feedback during rapid cipher manipulation while providing appropriate atmospheric enhancement across different learning phases.

The modular implementation architecture supports future expansion to additional cipher types while maintaining consistent educational quality and user experience patterns. The separation of educational content from technical implementation through JSON data structures enables rapid content iteration without compromising system stability, positioning the framework for continued development and educational content enhancement.

Chapter 5: Testing and Validation

5.1 Overview

This chapter presents the testing and validation results for Crypto Chronica, evaluating the system's functionality, educational content delivery, and user experience. Testing was conducted across seven critical domains: core cryptographic implementations, game progression systems, challenge phase mechanics, user interface design, data persistence mechanisms, content quality, and system performance.

The validation process employed systematic manual testing procedures to assess both technical functionality and educational content effectiveness (detailed checklist in Appendix A). Testing was performed under both fresh installation conditions and scenarios with existing save data, encompassing standard usage flows and stress conditions to identify potential stability issues.

The evaluation examined all major system components from fundamental cryptographic accuracy through complete user workflows spanning the entire learning progression. Results provide quantitative assessment through pass/fail metrics alongside qualitative evaluation of user experience factors, educational content quality, and system reliability under various operational conditions.

5.2 Testing Results

5.2.1 Core Cryptographic Functionality

Caesar Cipher Implementation

Tested: Basic encryption/decryption, alphabet wraparound, edge case handling, cipher wheel functionality

Results: 100% pass rate across all 7 test cases

Analysis: Implementation demonstrates mathematical accuracy with proper modular arithmetic for boundary conditions. Cipher wheel provides intuitive manipulation with real-time encryption preview. All edge cases including mixed character input and alphabet wraparound handled correctly.

Substitution Cipher Implementation

Tested: Key generation methods, drag-and-drop interface, frequency analysis integration

Results: 100% pass rate across all 9 test cases

Analysis: All key generation methods (random, keyword, Atbash) produce valid bijective mappings. Interactive substitution table demonstrates reliable drag-and-drop mechanics with appropriate conflict resolution. Frequency analysis tool provides accurate letter counting and meaningful cryptanalytic suggestions.

Pattern Analysis Tool

Tested: Frequency calculation accuracy, suggestion mechanisms, visual representation

Results: 100% pass rate across 3 test cases

Analysis: Tool accurately calculates letter frequencies and provides contextually appropriate suggestions for cipher breaking. However, effectiveness diminishes significantly with short text samples (under 25 characters), limiting utility for certain educational scenarios.

5.2.2 Game Progression System

Level Selection and Content Unlocking

Tested: Initial content availability, progression tracking, visual indicators

Results: 100% pass rate across 3 test cases

Analysis: Content gating functions correctly with Caesar and substitution ciphers appropriately accessible. Visual progress indicators clearly distinguish completed from available content. Phase transitions operate smoothly with proper context preservation.

Learn Phase Content Delivery

Tested: Historical content presentation, interactive demonstrations, navigation flow

Results: 100% pass rate across 4 test cases

Analysis: Historical narratives display effectively with seamless integration of interactive demonstrations. Cipher wheel components maintain full functionality within Learn phase contexts. Minor interference between demonstration components and text readability identified but does not impair educational effectiveness.

Practice Phase Exercise System

Tested: Exercise loading, tool integration, solution validation, hint delivery

Results: 100% pass rate across 4 test cases

Analysis: JSON-based exercise system loads correctly with clear task differentiation between encryption and decryption activities. Solution validation accurately recognizes correct answers across various input formats. Hint system provides appropriate guidance levels.

5.2.3 Challenge Phase System

Challenge Set Architecture

Tested: Set presentation, progress tracking, metadata display

Initial Results: 50% pass rate - inconsistencies in progress tracking and display functionality

Analysis: Challenge set presentation operates effectively with clear descriptions and appropriate difficulty indicators. However, initial testing revealed timing-sensitive state management issues during rapid scene transitions.

Resolution: Post-testing implementation of enhanced state validation and transition delays resolved inconsistencies

Final Status: System now maintains reliable progress tracking under normal and stress conditions

Individual Challenge Card Mechanics

Tested: Card progression, timer functionality, tool integration, context presentation

Initial Results: 50% pass rate - intermittent card lock state issues

Analysis: Core functionality operates correctly with proper tool integration and effective story context. Timer accumulation functions accurately across session boundaries.

Resolution: Enhanced state management eliminated timing sensitivity issues in card progression

Final Status: Reliable card progression with consistent unlock behavior

Challenge Completion and Validation

Tested: Answer validation, completion celebration, final progress recording

Results: 100% pass rate across 4 test cases

Analysis: Answer validation demonstrates appropriate flexibility in recognizing correct solutions while maintaining cryptographic accuracy. Completion feedback provides satisfying closure with accurate time recording and progress preservation.

5.2.4 User Interface and Experience

Audio System

Tested: Feedback mechanisms, contextual audio, volume levels, audio conflicts

Results: 100% pass rate across 4 test cases

Analysis: Audio feedback successfully enhances user experience without interference. Cipher tool manipulations generate contextually appropriate confirmation sounds. Polyphonic sound system prevents audio conflicts during rapid interactions.

Visual Design and Readability

Tested: Text clarity, element alignment, color contrast, visual hierarchy

Results: 50% pass rate - text contrast issues identified

Analysis: Overall layout and organizational elements demonstrate effective design with clear navigation pathways. However, insufficient text contrast against light backgrounds affects readability, particularly for users with varying visual capabilities. Font sizing remains appropriate but color scheme optimization needed.

Navigation and Control Systems

Tested: Back button functionality, escape key activation, navigation flow consistency

Results: 75% pass rate - timing sensitivity in rapid transitions

Analysis: Navigation operates reliably under normal conditions with appropriate consistency across application contexts. Minor timing-related issues identified during rapid interaction sequences, particularly during automatic advancement processes.

5.2.5 Data Persistence and System Reliability

Save/Load Functionality

Tested: Automatic progress saving, restoration accuracy, corruption handling

Results: 100% pass rate across 4 test cases

Analysis: Progress preservation operates reliably with transparent operation requiring no user intervention. System maintains data integrity through appropriate corruption protection while supporting accurate state restoration across session boundaries.

Timer Accuracy and Persistence

Tested: Challenge timer operation, pause functionality, time accumulation accuracy

Results: 100% pass rate across 4 test cases

Analysis: Timer functionality demonstrates precise operation with accurate pause/resume behavior during navigation sequences. Accumulated time values persist correctly across session interruptions while maintaining measurement precision during extended usage.

5.2.6 Content Quality and Educational Effectiveness

Historical Accuracy and Educational Content

Tested: Information verification, content presentation clarity, conceptual progression

Results: 100% pass rate across 2 test cases

Analysis: Educational content maintains historical accuracy with effective integration of contextual information and practical instruction. Interactive demonstrations successfully support conceptual understanding through hands-on manipulation.

Challenge Content Quality

Tested: Narrative engagement, puzzle solvability, difficulty progression, answer clarity

Results: 50% pass rate - accessibility concerns identified

Analysis: Challenge storylines demonstrate effective narrative engagement with historical plausibility. Most puzzles show clear solvability through systematic methodology. However, certain substitution cipher challenges present significant difficulty barriers for beginning users, requiring additional scaffolding or alternative solution pathways.

5.2.7 Performance and Stability

Normal Operation Performance

Tested: Frame rate stability, resource utilization, interface responsiveness

Results: 100% pass rate across 4 test cases

Analysis: System maintains smooth operation across target hardware configurations with consistent performance during extended sessions. Resource utilization remains within acceptable parameters without memory leaks or performance degradation.

Stress Testing and Edge Cases

Tested: Rapid input handling, large text processing, unusual interaction sequences

Results: 50% pass rate - edge case handling needs enhancement

Analysis: System demonstrates robust behavior under most stress conditions. Large text inputs process correctly without crashes. However, very rapid navigation during submission processes occasionally requires additional input validation to prevent unintended state changes.

5.2.8 Testing Results Summary

The testing evaluation produced quantitative results across all domains, demonstrating overall system effectiveness while identifying specific areas requiring attention. Table 5.1 presents core functionality testing results, indicating complete success in cryptographic implementation validation across all tested components.

Table 5.1: Core Functionality Testing Results

Component	**Test Category**	**Total Tests**	**Pass**	**Partial**	**Fail**	**Pass Rate (%)**	**Key Findings**
Caesar Cipher	Basic Encryption	4	4	0	0	100%	All mathematical operations correct
Caesar Cipher	Edge Cases	3	3	0	0	100%	Wraparound and character handling validated
Substitution Cipher	Key Generation	4	4	0	0	100%	All generation methods functional
Substitution Cipher	Interface Interaction	5	5	0	0	100%	Drag-and-drop mechanics reliable
Pattern Analysis	Frequency Analysis	3	3	0	0	100%	Accurate analysis and suggestions

Component	Test Category	Total Tests	Pass	Partial	Fail	Pass Rate (%)	Key Findings
Subtotal	**Core Functionality**	**19**	**19**	**0**	**0**	**100%**	**All core cryptographic functions operational**

The game progression system evaluation, summarized in Table 5.2, revealed mixed results with excellent performance in content delivery phases but notable issues in challenge phase state management that require attention.

Table 5.2: Game Progression System Testing Results

System Component	Test Category	Total Tests	Pass	Partial	Fail	Pass Rate (%)	Critical Issues
Level Selection	Unlock Mechanics	3	3	0	0	100%	Proper content gating
Learn Phase	Content Delivery	4	4	0	0	100%	Historical content presentation effective
Practice Phase	Exercise System	4	4	0	0	100%	Solution validation accurate

System Component	Test Category	Total Tests	Pass	Partial	Fail	Pass Rate (%)	Critical Issues
Challenge Hub	Set Selection	4	2	2	0	50%	Progress display inconsistencies
Challenge Cards	Card Mechanics	4	2	2	0	50%	Intermittent lock state issues
Challenge Cards	Solver Interface	5	5	0	0	100%	Tool integration successful
Challenge Sets	Completion System	4	2	2	0	50%	State management during submission
Subtotal	**Progression Systems**	**28**	**22**	**6**	**0**	**78.6%**	**Challenge phase requires stabilization**

User interface and experience testing results, presented in Table 5.3, demonstrate generally effective implementation with specific attention needed for visual accessibility enhancement.

Table 5.3: User Interface and Experience Testing Results

Interface Component	**Test Category**	**Total Tests**	**Pass**	**Partial**	**Fail**	**Pass Rate (%)**	**Notable Issues**
Audio System	Feedback Mechanisms	4	4	0	0	100%	Appropriate audio enhancement
Visual Design	Readability	4	2	2	0	50%	Text contrast issues identified
Navigation	Control Responsiveness	4	3	1	0	75%	Timing sensitivity in transitions
Interface Layout	Organization	4	4	0	0	100%	Clear visual hierarchy
Subtotal	**User Interface**	**16**	**13**	**3**	**0**	**81.3%**	**Visual contrast requires attention**

System reliability assessment, summarized in Table 5.4, confirmed robust data management with minor improvements needed for edge case handling.

Table 5.4: System Reliability Testing Results

Reliability Aspect	**Test Category**	**Total Tests**	**Pass**	**Partial**	**Fail**	**Pass Rate (%)**	**Performance Notes**
Data Persistence	Save/Load Functions	4	4	0	0	100%	Reliable progress preservation
Timer Accuracy	Challenge Timers	4	4	0	0	100%	Accurate time accumulation
Performance	Normal Operation	4	4	0	0	100%	Smooth performance maintained
Stability	Stress Testing	4	2	2	0	50%	Edge case handling needs improvement
Subtotal	**System Reliability**	**16**	**14**	**2**	**0**	**87.5%**	**Generally stable with minor edge cases**

Content quality and educational effectiveness evaluation, detailed in Table 5.5, demonstrated strong educational foundation with some accessibility considerations for challenge difficulty.

Table 5.5: Content Quality and Educational Effectiveness

Content Area	**Assessment Criteria**	**Total Tests**	**Pass**	**Partial**	**Fail**	**Pass Rate (%)**	**Educational Impact**
Historical Accuracy	Information Verification	2	2	0	0	100%	Historically accurate content
Educational Clarity	Content Presentation	2	2	0	0	100%	Clear learning progression
Challenge Quality	Narrative Engagement	2	2	0	0	100%	Engaging storylines
Puzzle Design	Solvability Assessment	2	1	1	0	50%	Some difficulty accessibility concerns
Subtotal	**Content Quality**	**8**	**7**	**1**	**0**	**87.5%**	**Strong educational foundation**

The overall testing summary, presented in Table 5.6, provides a full overview assessment across all evaluated domains.

Table 5.6: Overall Testing Summary

Testing Domain	**Total Tests**	**Pass Rate (%)**	**Critical Issues**	**Recommendation Priority**
Core Functionality	19	100%	None	Maintenance
Game Progression	28	78.6%	Challenge state management	High
User Interface	16	81.3%	Text contrast	Medium
System Reliability	16	87.5%	Edge case handling	Medium
Content Quality	8	87.5%	Difficulty accessibility	Low
Overall System	**87**	**86.2%**	**State management, UI contrast**	**Mixed priorities**

5.3 Critical Issues Analysis

Testing identified several issues requiring attention to ensure optimal user experience and system reliability. Issues are categorized by implementation priority based on their impact on core functionality and user experience.

5.3.1 High Priority Issues

Challenge Phase State Management

The most significant issue involved intermittent challenge card lock states that prevented user progression and required application restart for resolution. This occurred during rapid scene transitions, particularly during the submission and advancement process.

Resolution: Post-testing implementation of enhanced state validation and transition delays eliminated timing sensitivity issues. Additional state verification checkpoints now ensure proper state propagation before enabling navigation options.

Navigation Timing Sensitivity

Users attempting to navigate during automatic advancement sequences could inadvertently reset their progress, leading to frustration and potential learning session interruption.

Resolution: Implementation of confirmation dialogs and improved state management prevents accidental progress loss during rapid navigation sequences.

5.3.2 Medium Priority Issues

Visual Accessibility Limitations

Text contrast issues identified in certain interface elements where current color schemes provide insufficient contrast against light backgrounds, potentially affecting readability for users with varying visual capabilities.

Impact: Reduces accessibility for diverse user populations but does not prevent core functionality usage.

Recommendation: Systematic color scheme review to meet established accessibility standards.

Edge Case Handling

While the system demonstrates robust behavior under normal conditions, rapid input sequences and unusual interaction patterns occasionally require additional validation.

Impact: Affects system reliability under stress conditions but does not impact typical usage patterns.

Recommendation: Enhanced input validation and error handling for unusual interaction sequences.

5.3.3 Low Priority Enhancements

Challenge Difficulty Accessibility

Certain substitution cipher challenges present significant difficulty barriers for beginning users, potentially creating frustration for learners new to cryptographic concepts.

Impact: May affect learning progression for some users but does not prevent completion with appropriate persistence.

Recommendation: Additional scaffolding hints or alternative solution pathways for complex challenges.

Pattern Analysis Tool Limitations

Frequency analysis effectiveness diminishes with short text samples (under 25 characters), limiting utility for certain educational scenarios.

Impact: Reduces tool effectiveness in specific contexts but maintains educational value for appropriately sized content.

Recommendation: Enhanced analysis algorithms for short text or clear guidance on minimum text requirements.

5.4 Educational Effectiveness Assessment

The testing process validates Crypto Chronica's technical implementation and user interface functionality but reveals significant limitations in assessing actual educational effectiveness. This section acknowledges what the testing can and cannot determine about the system's pedagogical value.

5.4.1 Validated Educational Elements

Testing confirmed that historical narratives maintain factual accuracy with documented cryptographic development. Interactive demonstrations successfully integrate with educational explanations, providing hands-on experience with cryptographic principles. The three-phase progression structure operates as designed, guiding users from conceptual introduction through practical application.

All cryptographic implementations demonstrate mathematical precision with proper algorithm execution. Interactive tools maintain accuracy while providing intuitive interfaces, successfully bridging the gap between abstract mathematical concepts and practical manipulation. The system effectively tracks user engagement through completion rates, time-on-task measurements, and hint usage patterns. Challenge narratives demonstrate effective integration of historical context with problem-solving activities.

5.4.2 Educational Assessment Limitations

The testing methodology cannot determine whether game-based learning improves cryptographic understanding compared to traditional instructional methods. The evaluation lacks pre- and post-assessment learning measurements, comparative analysis with conventional cryptography education, and evaluation of knowledge retention over extended periods. Without controlled studies involving diverse user populations, the assessment cannot establish whether the interactive approach provides superior learning outcomes.

Testing involved limited user diversity, focusing primarily on technical functionality rather than educational accessibility across different age groups, learning preferences, and prior knowledge levels. The evaluation cannot determine effectiveness across varying cognitive styles or long-term retention patterns across different user types.

5.4.3 Pedagogical Framework Validation Gap

While the three-phase learning structure operates functionally, its educational effectiveness relative to alternative instructional approaches remains unvalidated. The assessment relied on subjective evaluation of content quality rather than objective measurement through established educational research protocols. This represents a fundamental distinction between functional operation and proven pedagogical effectiveness.

5.4.4 Educational Claims and Evidence Requirements

Based on testing results, the system can reliably claim to provide mathematically accurate cryptographic instruction, maintain historical authenticity, deliver engaging interactive experiences, and support systematic concept progression. However, claims regarding superior learning effectiveness, improved knowledge retention, enhanced motivation, or successful knowledge transfer require validation through formal educational research methodologies.

The distinction between technical implementation success and validated educational impact represents a critical gap in the current assessment. While Crypto Chronica demonstrates robust technical functionality and engaging user experience, its pedagogical value requires comprehensive educational effectiveness research to establish evidence-based claims about game-based cryptographic learning.

5.5 Discussion

The testing results reveal important insights about educational game development, technical implementation challenges, and the distinction between functional success and pedagogical validation. This section analyzes the broader implications of the findings for cryptographic education and interactive learning design.

5.5.1 Technical Implementation Success

The high pass rates for core cryptographic functionality (100%) and content delivery systems (87.5-100%) demonstrate that complex mathematical concepts can be successfully translated into interactive learning experiences while maintaining academic rigor. The Caesar cipher wheel's intuitive rotation mechanics and accurate real-time encryption preview exemplify effective educational interface design that makes abstract mathematical transformations feel naturally manipulable.

However, the substitution cipher implementation reveals a fundamental challenge in educational game design: creating interfaces that are both mathematically accurate and genuinely engaging. While the drag-and-drop table functions effectively for teaching letter mappings, it lacks the intuitive appeal of the cipher wheel, highlighting the difficulty of finding natural interaction paradigms for increasingly complex cryptographic concepts.

5.5.2 State Management and User Experience

The initial challenge phase issues (50% pass rate) and their subsequent resolution demonstrate both the value of systematic testing and the complexity of managing educational state across multiple interactive components. The timing sensitivity problems during scene transitions revealed that educational games require more robust state management than typical entertainment software due to the critical importance of preserving learning progress.

The successful resolution of these issues validates the iterative development approach, showing that comprehensive testing can identify real problems that significantly impact user experience. The enhanced state validation implementation now provides a stable foundation for complex educational interactions.

5.5.3 Educational Design Effectiveness

The three-phase learning progression demonstrates successful integration of tutorial, practice, and application elements. The 100% pass rate for Learn and Practice phases indicates that structured educational content delivery through interactive demonstrations effectively supports concept development. The Challenge phase's narrative-driven approach successfully contextualizes cryptographic problems within authentic historical scenarios.

However, the identified difficulty accessibility concerns (50% pass rate for challenge content quality) highlight the ongoing challenge of balancing educational rigor with learner support. Some substitution cipher challenges create significant barriers for beginning users, suggesting that educational games must carefully calibrate difficulty progression to maintain both challenge and accessibility.

5.5.4 Measurement and Validation Limitations

The testing results underscore a critical distinction between technical validation and educational effectiveness assessment. While the system demonstrates robust functionality and engaging user experience (86.2% overall pass rate), the absence of formal learning outcome measurement represents a significant limitation in establishing pedagogical claims.

This gap between technical implementation success and educational validation reflects broader challenges in educational technology development. The current testing validates that the system operates as designed and provides an engaging experience, but cannot determine

whether game-based learning improves knowledge retention compared to traditional cryptographic instruction.

5.5.5 Implications for Future Educational Game Development

The testing outcomes suggest several principles for educational game development. First, systematic testing must address both technical functionality and educational content quality from early development stages. Second, state management requires particular attention in educational contexts where progress preservation is critical to learning continuity. Third, interface design challenges increase significantly with conceptual complexity, requiring innovative approaches beyond conventional game mechanics.

The successful resolution of identified issues demonstrates that iterative development with comprehensive testing can produce reliable educational software. However, the educational effectiveness assessment gap indicates that future projects should incorporate formal learning research methodologies from the design phase rather than treating educational validation as a post-implementation consideration.

5.6 Conclusion

The systematic testing and validation process demonstrates that Crypto Chronica successfully achieves its technical objectives through mathematically sound cryptographic implementations and functionally effective content delivery mechanisms. The overall system pass rate of 86.2% across all tested domains indicates robust technical implementation with clearly identified areas for improvement.

Core cryptographic functionality achieved complete validation with 100% pass rates across all Caesar and substitution cipher implementations, confirming mathematical accuracy and proper algorithm execution. The three-phase learning progression operates reliably, delivering historical content effectively and supporting systematic concept development through interactive demonstrations and structured exercises.

The identification and resolution of challenge phase state management issues validates the effectiveness of comprehensive testing in educational software development. Initial problems with timing sensitivity during scene transitions were successfully addressed through enhanced state validation, demonstrating that iterative testing and improvement can produce stable educational systems capable of preserving critical learning progress.

However, the testing methodology employed has significant limitations in assessing actual educational effectiveness. While functional validation confirms that the system operates as designed and provides engaging user experiences, it cannot determine whether game-based cryptographic learning improves knowledge retention or understanding compared to traditional instructional methods. The absence of controlled learning outcome studies, comparative analysis with conventional teaching approaches, and diverse user population assessment represents a fundamental gap between technical validation and pedagogical effectiveness measurement.

The visual accessibility issues identified through testing highlight the importance of inclusive design in educational software. Text contrast improvements and enhanced edge case handling remain necessary to ensure optimal accessibility across diverse user populations and usage scenarios.

Testing confirms that Crypto Chronica provides a solid technical foundation for interactive cryptographic education, maintaining mathematical accuracy and historical authenticity while delivering engaging user experiences. The modular architecture and content management systems support future expansion and educational iteration. However, the educational impact claims require validation through formal educational research methodologies to establish evidence-based conclusions about the effectiveness of game-based cryptographic instruction.

With the identified technical improvements implemented and subsequent educational effectiveness research conducted, Crypto Chronica demonstrates significant potential as an interactive educational tool, establishing a foundation for future cryptographic education research while highlighting the careful distinction between technical implementation success and validated pedagogical impact.

Chapter 6: Conclusion

6.1 Introduction

This chapter presents the concluding analysis of the Crypto Chronica project, evaluating the implementation of an educational cryptography game designed to facilitate interactive learning of fundamental encryption concepts. The project demonstrates the practical application of game-based learning approaches to cryptographic education by developing a functional prototype that solves the challenges of making abstract cryptographic principles understandable through hands-on interactive activities.

The systematic development method used throughout this project has resulted in a technically solid educational tool that retains cryptographic accuracy while providing an engaging user experience. The three-phase learning progression approach, which includes historical context, interactive tools, and narrative-driven challenges, provides a framework for translating theoretical concepts into practical comprehension.

The following parts present a structured assessment of the project's outcomes. Section 6.2 compares outcomes to the original objectives outlined in Chapter 1. Section 6.3 explores the work's larger ramifications and significance in educational technology environments. Section 6.4 acknowledges the constraints and limitations that occurred during development and testing. Section 6.5 contains proposals for future improvements and research directions. Finally, Section 6.6 summarizes the overall contributions and situates the work in the larger framework of cryptographic education approach.

6.2 Objectives and Achievements

This section evaluates the project's success in meeting the three core objectives. Each objective is assessed through implementation evidence and testing outcomes.

6.2.1 Game Prototype with Historically Grounded Progression System

The first objective is to develop a game prototype that teaches cryptography concepts through a historically grounded progression system.

This objective has been successfully completed with the implementation of cipher types in chronological order, beginning with Caesar cipher (50s BCE) and advancing to Renaissance-era substitution ciphers. Historical content is integrated through narratives that provide authentic context for each cryptographic method.

The Learn Phase delivers historical scenarios including Julius Caesar's military communications and Renaissance diplomatic encryption. The progression system requires completion of fundamental concepts before unlocking advanced ciphers, ensuring systematic knowledge building. Testing confirmed proper content unlocking and accurate historical presentation across all implemented cipher types.

6.2.2 Effective Learning System with Tutorial and Progressive Elements

The second objective is to develop an effective learning system within the game that incorporates tutorial mechanisms, progressive difficulty scaling, and interactive puzzle-solving elements.

This objective is successfully completed through the three-phase learning structure. Tutorial mechanisms are implemented in the Learn Phase with interactive demonstrations including cipher wheel manipulation and substitution table construction. Progressive difficulty scaling

operates across phases (Learn > Practice > Challenge) and within phases through controllable parameters such as message length and hint availability.

The Practice Phase provides structured exercises with incremental complexity, while the Challenge Phase presents narrative-driven puzzles requiring concept synthesis. Testing confirmed accurate solution validation, effective hint delivery, and successful progression bridging from guided instruction to independent application.

6.2.3 Interactive Learning Framework with Effectiveness Measurement

The third objective is to create an interactive learning framework that teaches cryptographic fundamentals through game mechanics, measuring effectiveness through user completion data, and successful application of concepts in challenge scenarios.

This objective is successfully completed with comprehensive interactive tools and progress tracking. The framework includes specialized cryptographic tools (cipher wheel, substitution table, pattern analysis) that maintain mathematical accuracy while providing intuitive interfaces.

Game mechanics transform cryptographic concepts through challenge cards, timer systems, and achievement-based progression. The GameProgressManager captures completion data, exercise success rates, hint usage, and time-on-task measurements. Testing confirmed accurate data collection and solution validation across all learning activities.

However, the current implementation measures engagement and correct concept application but lacks comparative analysis to validate educational effectiveness against traditional methods.

6.3 Discussion

This section analyzes the broader implications of the Crypto Chronica implementation, examining its contributions to educational technology, cryptographic education methodology, and interactive learning design principles.

6.3.1 Educational Technology Contributions

The implementation shows how complex mathematical topics can be effectively converted into interactive learning experiences while maintaining academic rigor. The three-phase learning structure (Learn, Practice, and Challenge) provides a scalable approach for educational software development. This progression addresses different learning styles while maintaining clear advancement criteria, suggesting broader applicability beyond cryptographic education. The content management system enables rapid iteration on educational materials without heavy code modifications, supporting agile educational content development.

The integration of historical context and technical instruction reveals a successful strategy for motivating and engaging students in STEM education. By rooting abstract concepts in actual historical circumstances, the implementation demonstrates how narrative components can support rather than detract from technical learning objectives.

6.3.2 Cryptographic Education Methodology

Traditional cryptographic education often relies on theoretical presentations that may not adequately prepare students for practical application. Crypto Chronica addresses this gap by providing hands-on manipulation of cryptographic tools that mirror historical methods while maintaining mathematical accuracy.

The cipher tools implementation reveals the fundamental challenge of educational game design: creating interfaces that are both mathematically accurate and genuinely engaging. The Caesar cipher wheel successfully achieves this balance through intuitive rotation mechanics

that directly mirror the underlying mathematical transformation. However, the substitution table demonstrates the difficulty of this challenge—while functionally effective for teaching letter mappings, the drag-and-drop interface struggles to achieve the same level of natural engagement as the cipher wheel.

This design tension between educational effectiveness and engaging interaction becomes more pronounced with increasing cryptographic complexity. The implementation demonstrates that successful educational games require finding specific interaction paradigms that make abstract concepts feel naturally manipulable rather than merely functional.

The challenge system's narrative-driven approach provides realistic contexts for cryptographic problem-solving. Rather than isolated puzzles, learners encounter scenarios that demonstrate the practical applications and limitations of classical ciphers, building understanding of both technical methods and their historical significance.

6.3.3 Game-Based Learning Implementation

The implementation validates several principles of effective educational game design. The balance between educational content and game mechanics demonstrates that learning objectives can drive design decisions without compromising engagement. The hint system and progressive difficulty scaling show how scaffolding techniques can be integrated into game environments.

The testing results indicate that immediate feedback mechanisms and visual confirmation of correct actions significantly enhance the learning experience. Audio feedback integration provides additional reinforcement without overwhelming the primary visual learning channel, suggesting effective multi-modal design approaches.

6.3.5 Limitations and Research Implications

While the implementation successfully demonstrates technical feasibility and user engagement, the assessment of actual learning effectiveness remains incomplete. The testing methodology focused on functional validation rather than educational outcome measurement and user engagement, highlighting the distinction between technical success and pedagogical validation.

The current implementation measures completion rates and correct answer submission but cannot determine whether game-based learning improves knowledge retention compared to traditional methods. This limitation suggests that future educational software projects should incorporate formal learning assessment protocols from the design phase and with sufficient timing.

The project's scope limitation to desktop platforms may restrict accessibility for diverse learner populations. The interface design optimized for mouse and keyboard interaction may not effectively serve learners who would benefit from touch-based or mobile learning experiences.

6.4 Limitations and Constraints

This section acknowledges the limitations encountered during development and the constraints that influenced design decisions and project scope.

6.4.1 Educational Effectiveness Validation

The most significant limitation is the absence of formal educational effectiveness measurement. While the implementation successfully demonstrates technical functionality and some user engagement, it cannot establish whether game-based cryptographic learning improves knowledge retention or understanding compared to traditional instructional methods.

The testing methodology focused on functional validation rather than learning outcome assessment. Without controlled studies involving pre- and post-learning measurements, comparative analysis with conventional teaching methods, or long-term retention evaluation, the educational claims remain technically unvalidated despite positive user experience indicators.

6.4.2 Platform and Accessibility Constraints

The implementation only supports desktop platforms, limiting access for learners who would benefit from mobile or tablet-based learning experiences. The interface design optimized for mouse and keyboard interaction may not be appropriate for different user demographics, particularly those who require touch-based interfaces or alternate input methods.

Visual accessibility limitations were identified during testing, including insufficient text contrast in certain interface elements. These constraints may affect users with visual processing differences or varying display technologies, limiting the universal accessibility of the educational content.

6.4.3 Content Scope Limitations

The current implementation covers only Caesar cipher and simple substitution cipher methods. While this scope enables thorough exploration of fundamental concepts, it limits the breadth of cryptographic education that can be provided. Advanced topics such as polyalphabetic ciphers, mechanical encryption devices, or modern cryptographic principles remain outside the current framework.

This limitation stems from the inherent difficulty of adapting complex cryptographic methods into engaging gameplay mechanics. Even the implemented substitution table demonstrates the challenge of balancing educational effectiveness with engaging interaction - the drag-and-drop interface, while functional, struggles to maintain the intuitive engagement achieved by the Caesar cipher wheel. More complex ciphers like Vigenère or Enigma present significantly greater design challenges in creating interfaces that are both mathematically accurate and genuinely engaging rather than merely functional.

The historical context, while accurate for implemented ciphers, cannot provide comprehensive coverage of cryptographic development. Significant historical periods and cryptographic innovations are not addressed, limiting the complete historical narrative that could enhance understanding of cryptographic evolution.

6.4.4 Technical Implementation Constraints

Testing revealed state management issues in the challenge phase, particularly related to rapid scene transitions and submission processing. These technical constraints occasionally impact user experience and require system restarts to resolve, indicating limitations in the current architecture's robustness.

The JSON-based content management system, while enabling flexible content modification, requires technical understanding for complex interactive demonstrations. This constraint limits non-technical educators' ability to create sophisticated educational content without developer assistance.

6.4.5 Development Resource Constraints

As a proof-of-concept implementation, the project operated under typical academic development constraints including limited development time, single-developer implementation, and restricted testing resources. These constraints influenced design decisions toward demonstrating core functionality rather than comprehensive feature implementation.

The absence of diverse user testing populations limited the assessment of educational effectiveness across different age groups, educational backgrounds, and learning preferences. Resource constraints prevented extensive user studies that would provide more robust validation of the educational approach.

6.4.6 Research Methodology Limitations

The project's focus on technical implementation rather than educational research methodology resulted in limited data collection capabilities for learning assessment. While the system

captures completion metrics and interaction patterns, it lacks the instrumentation necessary for comprehensive educational effectiveness research.

The evaluation criteria emphasized technical functionality over pedagogical validation, reflecting the project's proof-of-concept nature but limiting claims about educational impact. Future research requiring controlled experimental design and educational assessment protocols would require different methodological approaches than those employed in this implementation.

6.4.7 Scalability and Maintenance Constraints

The current architecture, while modular, has not been validated for large-scale deployment or extended content libraries. Performance characteristics under high user loads or extensive content catalogs remain untested, limiting understanding of scalability requirements for broader educational deployment.

Maintenance requirements for educational content updates, technical platform evolution, and curriculum integration have not been thoroughly evaluated. These operational constraints may affect long-term viability in educational environments requiring ongoing support and content development.

6.4.8 Assessment Summary

These limitations and constraints provide important context for interpreting the project's achievements and contributions. While the implementation successfully demonstrates technical feasibility and engaging user experience design, the absence of formal educational validation limits definitive claims about learning effectiveness. The constraints identified point

toward necessary areas for future research and development to achieve comprehensive educational software validation.

6.5 Future Works and Recommendations

This section outlines specific recommendations for extending the Crypto Chronica framework, addressing identified limitations, and establishing comprehensive educational effectiveness validation.

6.5.1 Educational Effectiveness Research

The highest priority recommendation is implementing formal educational effectiveness studies to validate the game-based learning approach. Future research should include controlled experimental design comparing learning outcomes between Crypto Chronica and traditional cryptographic instruction methods.

Pre- and post-assessment protocols should examine knowledge retention, concept comprehension, and practical application skills across a variety of user demographics. S tudies measuring knowledge retention over time would provide critical information on the long-term viability of game-based cryptography learning in comparison to conventional methodologies.

A comparative analysis with existing educational tools and traditional textbook-based education would provide baseline effectiveness indicators. To guarantee that the conclusions are broadly applicable, these research should involve participants of various ages, educational backgrounds, and levels of prior cryptographic understanding.

6.5.2 Content Expansion and Interface Design Innovation

The modular architecture supports systematic expansion to additional cryptographic concepts, but this expansion requires solving fundamental interface design challenges rather than simply adding more content. Priority recommendations include developing engaging interaction

paradigms for polyalphabetic ciphers (Vigenère, Beaufort), mechanical encryption devices (Enigma machine simulation), and introductory modern cryptographic principles.

The critical challenge lies in creating interfaces that achieve the natural engagement of the Caesar cipher wheel rather than the more functional approach of the substitution table. Future cipher implementations must prioritize finding specific interaction metaphors that make complex mathematical operations feel intuitive and naturally manipulable. This may require innovative interface paradigms beyond traditional drag-and-drop or form-based approaches.

Research into educational game interface design should investigate how different cryptographic concepts can be translated into engaging physical metaphors. The success of the rotating cipher wheel suggests that interfaces mimicking historical tools may provide more natural engagement than abstract digital controls.

Each new cipher implementation should maintain the established three-phase learning structure while introducing appropriate complexity scaling. Historical context integration should continue providing authentic scenarios that demonstrate both the applications and vulnerabilities of each cryptographic method.

Curriculum mapping to established educational standards would support integration into formal educational programs. This includes developing assessment rubrics, learning objective alignment, and educator support materials that enable classroom adoption while maintaining educational flexibility.

6.5.3 Technical Platform Enhancement

Platform expansion to mobile and tablet devices would significantly improve accessibility and reach diverse learner populations. Touch-based interface adaptation should maintain the

intuitive manipulation characteristics of desktop tools while optimizing for smaller screen formats and gesture-based interaction.

Web-based deployment would eliminate installation barriers and enable broader accessibility across different operating systems and device configurations. Progressive web application architecture could provide offline capability while supporting cross-platform deployment.

Visual accessibility improvements should address identified contrast issues and implement comprehensive accessibility features including screen reader compatibility, keyboard navigation alternatives, and adjustable visual elements to serve learners with diverse accessibility requirements.

6.5.4 Advanced Learning Analytics

Enhanced data gathering capabilities should provide more detailed insights into learning patterns and performance measures. The use of learning analytics systems could track specific interaction patterns, problem-solving approaches, and concept mastery progression in order to inform both individual learning support and broader educational research.

Adaptive difficulty systems could change challenge complexity based on individual student performance patterns, resulting in tailored learning experiences that nonetheless meet educational objectives. Machine learning algorithms could use collected user data to determine optimal hint timing and content delivery strategies.

Real-time assessment integration could provide immediate diagnostic feedback to both learners and educators, enabling responsive educational support and intervention when learning difficulties are identified.

6.5.5 Collaborative Learning Features

Multi-user functionality could enable collaborative problem-solving experiences that mirror authentic cryptographic teamwork scenarios. Shared challenge spaces where learners work together on complex cryptographic problems would provide social learning opportunities while maintaining individual accountability.

Peer review systems could enable learners to share and evaluate challenge solutions, promoting deeper understanding through explanation and analysis of different problem-solving approaches.

6.5.6 Extended Challenge System Development

The narrative-driven challenge framework should be expanded with additional historical scenarios covering different time periods and cryptographic applications. Medieval manuscript protection, World War communication security, and Cold War intelligence scenarios could provide diverse contexts for applying cryptographic skills.

Procedural challenge generation could create unlimited practice opportunities while maintaining educational quality and appropriate difficulty scaling. Algorithm-driven scenario creation could provide fresh challenges that maintain narrative coherence while offering varied problem-solving experiences.

Integration with historical databases and primary source materials could enhance authenticity while providing research opportunities that combine cryptographic skills with historical investigation methods.

6.5.7 Performance and Scalability Optimization

Large-scale deployment validation should assess system performance under multiple concurrent users and extensive content libraries. Load testing and performance optimization would ensure reliable operation in educational environments with significant user populations.

Content management system enhancement should enable non-technical educators to create sophisticated interactive demonstrations and challenges. Visual content creation tools could empower domain experts to develop educational materials without requiring programming expertise.

Automated testing frameworks should ensure continued functionality as content and features expand, supporting sustainable development practices that maintain educational quality while enabling rapid content iteration.

6.6 Summary

This chapter has evaluated the Crypto Chronica project, examining its achievements, contributions, limitations, and future directions within educational cryptography game development.

The project successfully achieved all three established objectives, creating a functional educational game prototype that integrates cryptographic instruction with historical context through a three-phase learning progression. The implementation demonstrates that complex mathematical concepts can be translated into interactive learning experiences while maintaining cryptographic accuracy and historical authenticity.

The technical implementation produced significant contributions to educational technology. The modular architecture enables rapid educational material iteration, while the three-phase learning structure provides a scalable framework applicable beyond cryptographic education. The JSON-based content management system supports collaborative development between technical implementers and domain experts.

However, the project revealed fundamental challenges in educational game design, particularly the tension between mathematical accuracy and genuinely engaging interaction. While the Caesar cipher wheel achieves natural, intuitive manipulation, the substitution table demonstrates the difficulty of creating equally engaging interfaces for more complex concepts. This insight highlights that expanding educational games requires solving interface design challenges rather than simply adding content.

Testing validation confirmed robust technical functionality with an overall system pass rate of 86.2%, though specific issues in challenge phase state management and visual accessibility require attention.

The most significant limitation is the absence of formal educational effectiveness validation. While the implementation demonstrates technical functionality and engaging user experience, it cannot establish whether game-based cryptographic learning improves knowledge retention compared to traditional methods. This distinguishes between technical implementation success and validated educational impact.

The project's scope limitation to Caesar and substitution ciphers reveals the broader challenge of adapting complex cryptographic methods into engaging gameplay mechanics, presenting both a design challenge and research opportunity.

Future work priorities include formal educational effectiveness research through controlled studies, platform expansion to mobile devices, and innovative interface design approaches that achieve the natural engagement demonstrated by the Caesar cipher wheel.

Crypto Chronica represents a successful proof-of-concept for game-based cryptographic education, demonstrating that interactive learning frameworks can maintain educational rigor while providing engaging experiences. The project contributes valuable insights into educational game design challenges and establishes a foundation for future cryptographic instruction research, positioning game-based learning as a viable approach while highlighting the careful balance required between technical accuracy, historical authenticity, and genuine user engagement.

References

Cohen, E. A., & Kahn, D. (1997). The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. *Foreign Affairs*, *76*(3), 129. https://doi.org/10.2307/20048054

Cohen, E. A., & Singh, S. (1999). The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography. *Foreign Affairs*, *78*(6), 148. https://doi.org/10.2307/20049567

CryptoClub. (n.d.). https://cryptoclub.org/

Cypher on Steam. (n.d.). https://store.steampowered.com/app/746710/Cypher/

Dave. (2024, March 10). Understanding Classical cryptography. *CodedInsights*. https://codedinsights.com/classical-cryptography/overview/

Frequency Analysis - 101 Computing. (2022, February 7). *101 Computing - Boost Your Programming Skills!* https://www.101computing.net/frequency-analysis/

Godot Docs – 4.4 branch. (2025). Godot Engine Documentation. https://docs.godotengine.org/en/stable/

Gui, Y., Cai, Z., Yang, Y., Kong, L., Fan, X., & Tai, R. H. (2023). Effectiveness of digital educational game and game design in STEM learning: a meta-analytic review. *International Journal of STEM Education*, *10*(1). https://doi.org/10.1186/s40594-023-00424-9

Jin, G., Tu, M., Kim, T., Heffron, J., & White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning (EduLearn)*, *12*(1), 150–158. https://doi.org/10.11591/edulearn.v12i1.7736

Keep Talking and Nobody Explodes - Defuse a bomb with your friends. (2023, October 10). Keep Talking and Nobody Explodes. https://keeptalkinggame.com/

Savarese, C., & Hart, B. (2010). *Caesar Cipher*. https://www.cs.trincoll.edu/~crypto/historical/caesar.html

Shakhmalova, I., & Zotova, N. (2023). Techniques for increasing educational motivation and the need to assess students' knowledge: The Effectiveness of Educational Digital Games in learning English Grammatical material. *Journal of Psycholinguistic Research*, *52*(5), 1875–1895. https://doi.org/10.1007/s10936-023-09983-y

Simmons, & J, G. (2025, May 13). *Cryptology | Definition, Examples, History, & Facts*. Encyclopedia Britannica. https://www.britannica.com/topic/cryptology/History-of-cryptology

Spillman, R., Janssen, M., Nelson, B., & Kepner, M. (1993). USE OF a GENETIC ALGORITHM IN THE CRYPTANALYSIS OF SIMPLE SUBSTITUTION CIPHERS. *Cryptologia*, *17*(1), 31–44. https://doi.org/10.1080/0161-119391867746

Telsy. (2022, April 22). *Al-Kindi, the father of cryptanalysis*. Telsy. https://www.telsy.com/en/al-kindi-the-father-of-cryptanalysis/

Tharot, K., Riel, A., & Thiriet, J. (2024). A gamification approach to teaching Cybersecurity in CPS. *Procedia CIRP*, *128*, 799–803. https://doi.org/10.1016/j.procir.2024.06.039

The Babington Plot. (2024). Spartacus Educational. https://spartacus-educational.com/TUDbabingtonP.htm

Wikipedia contributors. (2025, June 21). *Caesar cipher*. Wikipedia. https://en.wikipedia.org/wiki/Caesar_cipher

Appendix A

Crypto Chronica Manual Testing Checklist

Testing Information

- Tester Name: _____
- Testing Date: _____
- Platform: _____
- Device/OS: _____

1. CORE CIPHER FUNCTIONALITY

Caesar Cipher Tests

Test 1.1: Basic Caesar Encryption

Pre-conditions:

- Game launched
- Navigate to Practice Phase → Caesar Cipher

Requirements:

- Cipher wheel rotates smoothly
- Shift values display correctly (0-25)
- Encryption preview updates in real-time

Test Steps:

1. Set cipher wheel to shift 3
2. Enter "HELLO" in workspace
3. Observe encryption preview

Expected Results:

- Wheel shows "Shift: 3"
- Preview shows correct shifted letters

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Test 1.2: Caesar Cipher Edge Cases

Pre-conditions:

- Caesar cipher wheel available

Requirements:

- Handles wraparound correctly (X→A, Y→B, Z→C)
- Preserves spaces and punctuation
- Handles both uppercase and lowercase input

Test Steps:

1. Set shift to 3
2. Test "XYZ 123!"
3. Test "hello world"

Expected Results:

- "XYZ 123!" → "ABC 123!"
- "hello world" → "KHOOR ZRUOG" (or similar formatting)

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Substitution Cipher Tests

Test 1.3: Substitution Table Generation

Pre-conditions:

- Navigate to Practice Phase → Substitution Cipher

Requirements:

- Random key generation works
- Keyword generation works
- Atbash generation works
- Manual letter mapping works

Test Steps:

1. Click "Generate Random"
2. Click "Generate from Keyword" with "CIPHER"
3. Click "Atbash"

4. Manually change A→X

Expected Results:
- Each generation creates different, complete mappings
- Keyword starts with C-I-P-H-E-R
- Atbash shows A→Z, B→Y, etc.
- Manual changes update preview

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Test 1.4: Frequency Analysis Tool
Pre-conditions:
- Substitution cipher tools available

Requirements:
- Analyzes letter frequency correctly
- Provides meaningful suggestions
- Visual bars represent frequency accurately

Test Steps:
1. Enter encrypted text: "WKH TXLFN EURZQ IRA"
2. Click "Analyze"
3. Check frequency bars and suggestions

Expected Results:
- Most frequent letters highlighted
- Suggestions like "W→T" based on frequency
- Bars show relative frequencies

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

2. GAME PROGRESSION SYSTEM

Test 2.1: Level Selection and Unlocking

Pre-conditions:

- Fresh game start or known progress state

Requirements:

- Caesar cipher always unlocked
- Substitution cipher unlocked from start
- Progress indicators work correctly

Test Steps:

1. Open Level Selection
2. Check which ciphers are unlocked
3. Check if all phases are unlocked

Expected Results:

- Clear visual indication of locked/unlocked content
- Progress updates after completion
- Appropriate phase transitions

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Test 2.2: Learn Phase Navigation

Pre-conditions:

- Access to Learn Phase (any cipher)

Requirements:

- Historical content displays correctly
- Demo tools work interactively
- Navigation between pages smooth
- Progress saves correctly

Test Steps:

1. Start Learn Phase for Caesar
2. Navigate through all pages
3. Interact with cipher wheel demo
4. Complete the phase

Expected Results:
- All historical text readable
- Interactive demos respond correctly
- "Complete" button works
- Progress marked as completed

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Test 2.3: Practice Phase Exercises
Pre-conditions:
- Access to Practice Phase

Requirements:
- Exercises load correctly
- Hints system works
- Solution checking accurate
- Progress between exercises

Test Steps:
1. Complete first practice exercise
2. Use hint system
3. Submit correct answer
4. Progress to next exercise

Expected Results:
- Exercise instructions clear
- Hints provide helpful information
- Correct answers accepted
- Smooth progression to next exercise

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

3. CHALLENGE PHASE

Test 3.1: Challenge Set Selection

Pre-conditions:

- Access to Challenge Hub

Requirements:

- Challenge sets display correctly
- Difficulty indicators accurate
- Estimated time shown
- Progress indicators work

Test Steps:

1. Access Challenge Hub
2. Review available challenge sets
3. Select a challenge set
4. Check set information display

Expected Results:

- Clear set descriptions
- Appropriate difficulty levels
- Time estimates reasonable
- Progress from previous attempts visible

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Test 3.2: Challenge Card Mechanics

Pre-conditions:

- Challenge set loaded

Requirements:

- Cards display locked/unlocked correctly
- Card progression follows unlock conditions
- Timer functions properly
- Context information helpful

Test Steps:
1. Start "Merchant Conspiracy" challenge set
2. Complete first card
3. Check if second card unlocks
4. Monitor timer functionality

Expected Results:
- Initial card unlocked, others locked
- Completion unlocks next card
- Timer runs continuously
- Context provides story immersion

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Test 3.3: Card Solver Interface
Pre-conditions:
- Individual challenge card opened

Requirements:
- Cipher tools available and functional
- Hint system provides guidance
- Answer validation works correctly
- Return navigation preserves progress

Test Steps:
1. Open a challenge card
2. Use available tools to solve
3. Submit incorrect answer
4. Use hints
5. Submit correct answer

Expected Results:
- Tools function same as practice phase
- Incorrect answers provide feedback
- Hints guide toward solution

- Correct answers register completion

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Test 3.4: Challenge Set Completion
Pre-conditions:
- All cards in a set completed

Requirements:
- Main question becomes available
- Final answer validation works
- Completion celebration appropriate
- Progress saves correctly

Test Steps:
1. Complete all cards in a challenge set
2. Answer main question
3. Submit final answer
4. Check completion dialog

Expected Results:
- Main question clearly presented
- Final answer validation accurate
- Satisfying completion feedback
- Set marked as completed

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

4. USER INTERFACE & EXPERIENCE

Test 4.1: Audio System

Pre-conditions:

- Audio enabled in system

Requirements:

- UI sounds play on interactions
- Audio provides appropriate feedback
- Volume levels appropriate
- No audio glitches or overlaps

Test Steps:

1. Navigate through menus
2. Interact with cipher tools
3. Complete various actions
4. Test rapid clicking

Expected Results:

- Clear audio feedback for all interactions
- Sounds enhance experience without annoyance
- No audio cutting out or overlapping
- Audio scales appropriately with actions

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Test 4.2: Visual Design & Readability

Pre-conditions:

- Game running at target resolution

Requirements:

- Text clearly readable at all sizes
- UI elements properly aligned
- Color contrast sufficient
- Visual hierarchy clear

Test Steps:

1. Review all major screens
2. Check text readability
3. Verify button/element alignment
4. Test on different screen sizes if possible

Expected Results:

- All text easily readable
- UI elements properly positioned
- Good contrast between text and backgrounds
- Clear visual organization

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Test 4.3: Navigation & Controls

Pre-conditions:

- Game accessible

Requirements:

- Back buttons work from all screens
- Navigation flow logical and intuitive
- Escape key brings up exit menu
- No dead-end screens

Test Steps:

1. Navigate through all major game areas
2. Use back buttons from various screens
3. Test Escape key functionality
4. Verify you can always return to main menu

Expected Results:

- Consistent navigation experience
- All back buttons function correctly
- Escape menu accessible from gameplay
- Clear path back to main menu

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

5. DATA PERSISTENCE & RELIABILITY

Test 5.1: Save/Load Functionality

Pre-conditions:

- Fresh game start

Requirements:

- Progress saves automatically
- Progress loads correctly on restart
- No progress loss during normal gameplay
- Save file handles corruption gracefully

Test Steps:

1. Make progress in game (complete some phases)
2. Exit and restart game
3. Verify progress maintained
4. Test with rapid exits

Expected Results:

- All progress correctly restored
- No loss of completed content
- Game handles unexpected exits gracefully
- Save system works transparently

Status: ☐ Pass ☐ Fail ☐ Partial

Remarks: _____

Test 5.2: Timer Accuracy

Pre-conditions:

- Challenge sets available

Requirements:
- Timers start/stop/pause correctly
- Time accumulates accurately
- Timer persists through scene changes
- Final times displayed correctly

Test Steps:
1. Start a challenge set
2. Work on challenges
3. Exit and return to set
4. Complete set and check final time

Expected Results:
- Timer runs only during active work
- Time pauses during card solving
- Accurate time accumulation
- Reasonable final completion times

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

6. CONTENT VALIDATION

Test 6.1: Historical Accuracy & Educational Value
Pre-conditions:
- Access to Learn phases

Requirements:
- Historical information accurate
- Educational content clear and informative
- Examples support learning objectives
- Progression builds knowledge appropriately

Test Steps:
1. Review historical content in Learn phases
2. Check accuracy of cipher examples
3. Evaluate educational clarity

4. Assess knowledge building

Expected Results:
- Historically accurate information
- Clear educational explanations
- Examples reinforce concepts
- Logical knowledge progression

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Test 6.2: Challenge Content Quality
Pre-conditions:
- Access to challenge sets

Requirements:
- Stories engaging and coherent
- Cipher puzzles solvable
- Difficulty progression appropriate
- Answers clearly correct

Test Steps:
1. Play through complete challenge sets
2. Evaluate story quality and engagement
3. Verify puzzle solvability
4. Check answer accuracy

Expected Results:
- Engaging, coherent storylines
- All puzzles have clear solutions
- Appropriate difficulty scaling
- Unambiguous correct answers

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

7. PERFORMANCE & STABILITY

Test 7.1: Performance Under Normal Use

Pre-conditions:

- Target hardware/software environment

Requirements:

- Smooth performance during normal gameplay
- No significant frame rate drops
- Responsive user interface
- Reasonable memory usage

Test Steps:

1. Play through extended session
2. Use all major features
3. Monitor performance
4. Check for slowdowns

Expected Results:

- Consistent smooth performance
- UI remains responsive
- No noticeable memory leaks
- Stable frame rates

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

Test 7.2: Stress Testing

Pre-conditions:

- Game loaded

Requirements:

- Handles rapid input without crashes
- Large text inputs processed correctly
- Multiple rapid scene transitions stable
- Recovery from unexpected situations

Test Steps:

1. Rapidly click various UI elements
2. Enter very long text in input fields
3. Quickly navigate between screens
4. Test edge cases and unusual inputs

Expected Results:

- No crashes from rapid input
- Graceful handling of large inputs
- Stable scene transitions
- Appropriate error handling

Status: [ ] Pass [ ] Fail [ ] Partial

Remarks: _____

OVERALL TEST SUMMARY

Critical Issues Found:

_____

_____

Minor Issues Found:

_____

_____

Recommendations:

_____

_____

Overall Assessment:

[ ] Ready for Release

[ ] Minor Issues - Release with Notes

[ ] Major Issues - Requires Fixes

[ ] Not Ready - Significant Problems

Tester Signature: _____ Date: _____