



CIPHERCRAFT

Specification Document

Author

Josh Casey
C00261828

Table Of Contents

Introduction:	4
Purpose:	4
Audience:	5
Use Case.....	6
Actors.....	7
User:.....	7
Admin:.....	7
Use Case Descriptions.....	8
CipherCraft Course Overview.....	11
Module 1: The Start of Cryptograph.....	11
Module 2: Where it is now.....	12
Module 3: Advanced Encryption Standard (AES)	13
Module 4: Hashing Algorithms.....	14
Module 5: Key Management.....	15
Deliverables	16
Development Core Deliverables.....	16
Account Management:	16
Interactive Learning:.....	16
User Profile & Progress Tracking:	17
Assessment System:	17
Material Visual & Written:	18
Graphical User Interface (GUI):	18
Admin Control Panel:.....	18
Document Core Deliverables	19
Specification Document:.....	19
Research Document:.....	19
Research Poster:.....	19
Presentation:	19
Final Document:	19
Non-Core Deliverables.....	20
Lab Instructions:	20
Additional Educational Resources:	20

User Feedback:	20
Gamification:	21
Discussion Board:.....	21
Technologies	22
Languages: Python, HTML, CSS, JavaScript	22
Python:.....	22
HTML:.....	22
CSS:	23
JavaScript:	23
Framework: Flask, Django.....	24
Flask:	24
Django:.....	24
Tools: Visual Studio Code, XAMPP, GitHub.....	25
Visual Studio Code:	25
XAMPP:	25
GitHub:.....	25
Database: MySQL, Docker.....	26
MySQL:	26
Docker:.....	26
Interface Design	27
Login / Sign up Page.....	28
Dashboard / Main Page	30
Course Page.....	31
Quiz Page	32
Lab Page.....	33
Profile Page	34
Metrics.....	35
FURPS.....	36
Functionality:.....	36
Usability:	36
Reliability:	37
Performance:.....	37
Supportability:.....	37

Project Plan 38
References 39

Introduction:

CipherCrafts mission is to create a web-based application that will provide a starter curriculum in cryptography. The platform is designed as a gateway, allowing students on their journey of computing, to gain a rudimentary understanding of cryptography. The value of cryptography cannot be exaggerated, from securing bank transactions to private communications it makes them all possible. cryptography has forged its name in history (UseOfCrypto).

Online methods of learning are provided free with websites such as CrypTool, CryptoPals, and Hack The Box, offering assistance and material with separate approaches to teaching. CrypTool for example, offers a range of downloadable applications that are open source and supply different teaching methods (CrypTools). While CryptoPals challenges the users with tasks related to cryptography, it focuses more on the implementation of cryptographic methods (CryptoPals).

CipherCraft plans to follow in their footsteps by providing a free online platform that teaches cryptography. However, CipherCraft will contrast with the aforementioned tools by focusing more at a beginner's level, offering a starting point, and providing engagement through interactive experience. The use of meticulously crafted quizzes will aid in assessing the knowledge gained by the users.

This document will outline the functions of CipherCraft, how the users can interact with the platform, a description of the curriculum, and a more in-depth detailed description of the modules intended. A template design for the platform so a general idea of its aesthetic can be seen, a use case with detailed user interactions. The document aims to aid how the application will function when development is complete.

Purpose:

CipherCraft's purpose is to create a free online pathway for those intrigued by cryptography, allowing them to find a foothold in this vast and complex topic. More specifically, CipherCraft aims to support third-level education students, mainly those in the computing sector such as Cyber Security, Software Development, IT Management, and others. The focus on these students is to provide an insight into the world of cyber security allowing them to gain knowledge on a subject that is present in most areas of cyber security.

It will provide an interactive approach allowing the users to engage with the platform and learn from practical methods. This will help create an enjoyable experience for the user. While progress tracking will help track their progress it helps the users gauge their understanding of cryptography. Allowing them to view their improvements with quizzes.

CipherCraft will not only provide the users with theoretical knowledge but also practical skills related to cryptography. The platform plans on having hands-on exercises and tasks that will provide the users with the ability to apply cryptographic techniques in the real world.

Audience:

The online platform will be primarily aimed at those starting their third-level education journey in computing. It will provide them with both the purpose and history of cryptography while delving into the fundamentals of different algorithmic techniques. This will allow the students to grasp an interesting and complex topic.

As cryptography is a major aspect of cyber security the platform is targeted towards students pursuing a degree in cyber security, allowing for them to understand the essentials of cryptography. Equipping them with the knowledge needed for their course, as cryptography is involved in many different topics such as networking, web security, and many more it is continuously used and mentioned throughout.

The platform is also valuable to students who are studying software development and programming as it will provide information on how to secure software and data. The knowledge they learn will explain the importance and practical methods of how to use simple encryption methods as well as exploring cyber security as a possible career path.

Students studying IT Management may utilize the platform as it will benefit them by integrating the different principles and methods learned from CipherCraft, such as informed decisions about data protection. As it only teaches the basics they will be able to grasp an understanding of cryptography and how the process works.

As the content focuses on a starting point for learning cryptography it allows the users to delve deeper into the vast topic and explore their interest in cyber security. It provides them with knowledge and understanding of what cryptography is and how it will benefit them as well as being able to implement different encryption techniques.

Use Case

The use case diagram below was created using Draw.io, it demonstrates how a user and administrator may interact with the application. See “

Actors” for more information about the User and Admin, and “Use Case Descriptions” for more information about the use cases.

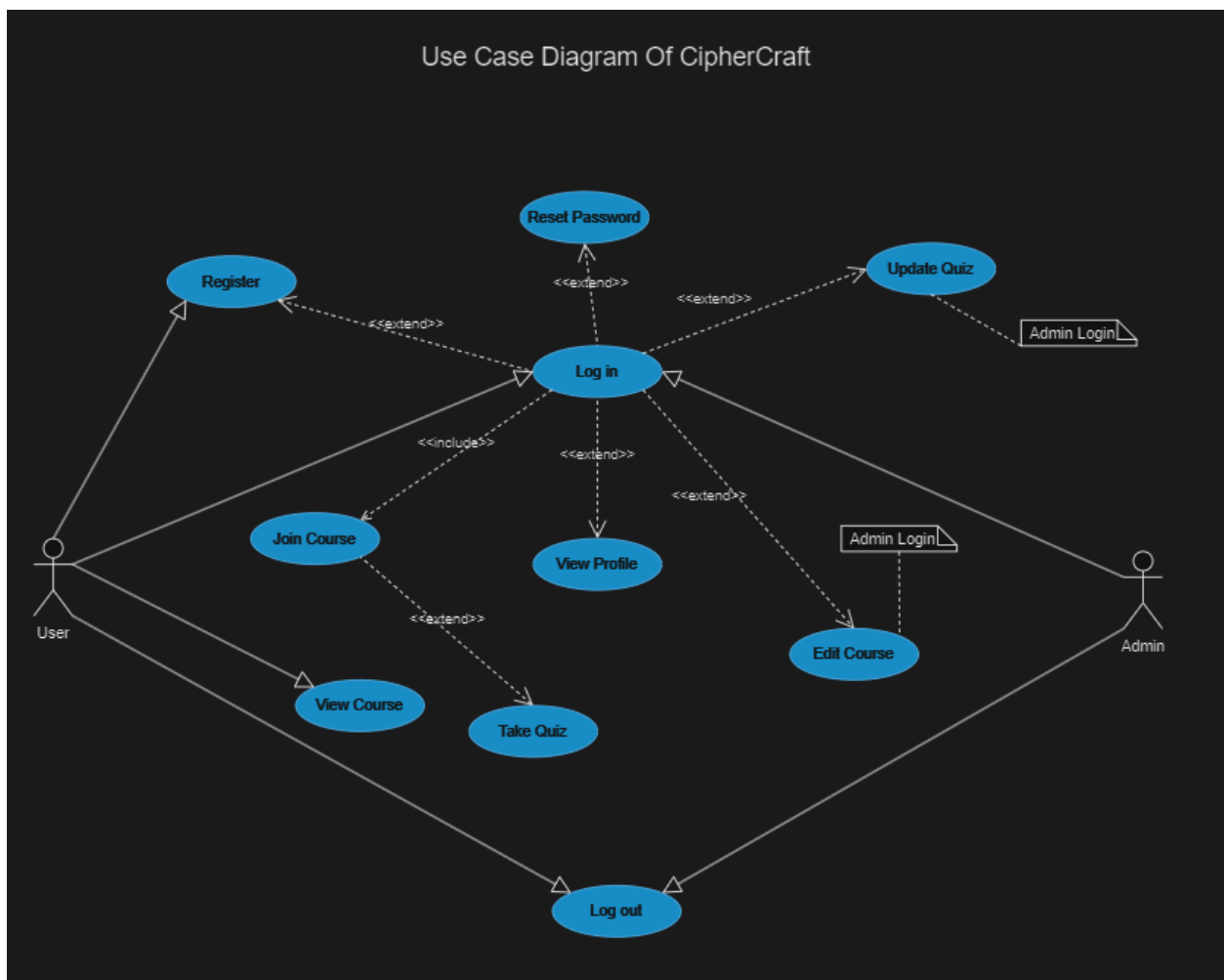


Figure 1: Use-Case Diagram of CipherCraft

Actors

User:

Users of the platform are able to create an account, login with the details they provided, change their password if they have forgotten or wish to strengthen it, view the details of the course, so they have a general idea of what they will learn. They will also be able to join the course if they think it will benefit them, take part in the quizzes so they may progress to the next level. Users will also be able to view their own profile, so they can view their journey on CipherCraft. When a user is finished with CipherCraft for the day they will also be able to log out of there account.

Admin:

The administrator account is made so any changes that may be required can be done so. The admin is able to login, change their password if they think it has been compromised, or in need of an update, view there profile to see what privileges they have. Admins are able to alter the content of the web page if any inconsistency are found, or is future findings end up changing the knowledge presented on the page. Admins will also be able to update the quizzes incase the questions are found to be too difficult or easy. Once the admin is finished with all of their tasks they can then logout.

Use Case Descriptions

Name	Register
Actors	User
Description	Creating an account to, join course and store progress
Precondition	Have a valid email address
Main success scenario	User provides valid details and creates an account to further use the platform
Postcondition	The user is brought to the home page

Name	Login
Actors	User, Admin
Description	Logging into existing account
Precondition	Valid credentials
Main success scenario	Logs the account in to the correct account with the correct detail
Postcondition	User is brought to the home page

Name	Join Course
Actors	User
Description	The view the material, and become more knowledgeable about cryptography
Precondition	Logged in to account
Main success scenario	User is able to view the material of the course and begin learning
Postcondition	User can start viewing the modules material

Name	Take Quiz
Actors	User
Description	To progress to the next module
Precondition	Completed module
Main success scenario	User can answer questions in the quiz and progress to the next module if successful
Postcondition	User can start and finish quiz once module is complete

Name	View Profile
Actors	User, Admin
Description	View progress/privileges
Precondition	Logged in to account
Main success scenario	Correct information about the account can be viewed
Postcondition	That the information can be viewed is true and correct to the account logged in

Name	Edit Course
Actors	Admin
Description	To make changes to the courses content in case of inconsistency's, errors, etc..
Precondition	Logged in as admin
Main success scenario	That the information can be viewed, altered and updated
Postcondition	That the information is updated

Name	Update Quiz
Actors	Admin
Description	To make the questions simpler or harder
Precondition	Logged in as admin
Main success scenario	That the questions can be viewed, altered and updated
Postcondition	That the questions are updated

Name	Reset Password
Actors	User, Admin
Description	To change forgotten password, strengthen previous password, etc.,
Precondition	Have a valid account
Main success scenario	That the password is changed and updated
Postcondition	Password has been updated

Name	View Course
Actors	User, Admin
Description	The see what content will be covered on the platform. (Home Page)
Precondition	Viewing home page
Main success scenario	That the information about the course is visible and true
Postcondition	That the course details provided are true and correct

Name	Logout
Actors	User, Admin
Description	Allows the person to safely logout of their account.
Precondition	Logged in to account
Main success scenario	The account is logged out of and the information is stored, and not visible until user logs back in
Postcondition	Brought back to the main page of platform

CipherCraft Course Overview

CipherCraft curriculum is based upon five different modules, each module will bring the user closer and closer to achieving a fundamental knowledge about cryptography. Each module must be complete before progressing to the next level. After each module a lab will be provided for the user so they can obtain hands on experience with cryptography. A quiz will be mandatory after each module, this will ensure that the user has gained knowledge and understanding from each module. A module description and breakdown is provided below:

Module 1: The Start of Cryptograph

Topics:

- Why it began?
 - o Brief History of why cryptography was invented
- Caesar Cipher
 - o Method of encrypting, decrypting, the use of a key
- Vigenère Cipher
 - o Method of encrypting, decrypting
- Fence Cipher
 - o Method of encrypting, decrypting

Breakdown:

The first module shall contain a brief history of cryptography and why it was brought about. As history is a very important aspect of any and all subjects. It will contain a brief description of different terminology used throughout the course so that the users do not begin to feel lost in later stages. Module one will also contain some ciphers from the past so users can see how they work and function so they have a general idea as to how an encryption process works.

Encryption systems from the past that will be covered and shown are the Caesar Cipher, Vigenère Cipher, and the Fence Cipher. Each cipher will follow this general approach:

- What the encryption process entails
- What the decryption process entails
- The methods to encrypt and decrypt

Each encryption process will also include an interactive, aspect so that the users can engage with the platform and view a better understanding through visual methods. For example, the user will be prompted to enter text to encrypt and it will output the ciphertext.

Module 2: Where it is now

Topics:

- Symmetrical & Asymmetrical
 - o What they are, the differences
- Block Ciphers & Stream Ciphers
 - o The differences, how they work
- One-Time Pad
 - o Explaining XOR and demonstrating it
- Methods of Key Exchange
 - o Diffie-Hellman key exchange protocol

Breakdown:

Module two will go into more detail about the different types of encryption methods that are used nowadays, such as the type of encryptions so the users will understand the breakdown of cryptography more. Such as symmetric and asymmetric how they both operate, how they contrast each other, the advantages and disadvantages of each.

Providing an overview of the different types of data encryptions such as block ciphers and stream ciphers, what they are used for, how they are used. Use of visuals to demonstrate how these methods operate and function. When and where you may see these encryptions being used.

One-Time pad as an example of perfect encryption, how its work, demonstrating XOR so the understanding can be used later in the more advanced encryption methods. This module will contain an interactive section allowing for the user to work with XOR. Explain how One-Time pad is not achievable in the real world.

Diffie-Hellman key exchange protocol will be used as an example of how to securely exchange keys for communication purpose. It will explain the importance of being able to exchange keys without a third party individual knowing the key. The process will be detailed through visual and interactive methods.

Module 3: Advanced Encryption Standard (AES)

Topics:

- AES Process
 - Showing how AES functions
- Electronic Codebook (ECB) Mode
 - Example of a bad mode of encryption
- Cipher Block Chaining (CBC) Mode
 - Strong mode of encryption
- Counter (CTR) Mode
 - Mode used the most

Breakdown:

Module three will provide an in-depth break down of how the AES encryption functions i.e., the number of rounds, sub bytes, shift rows, mix columns, etc. This will allow the user to gain a more in-depth understanding of symmetric encryption, when and why it is used, how it is used. Providing an interactive section where the user can enter the text they wish to encrypt and the key, showing how the encryption works.

Explain how AES has multiple modes of operation allowing to make the encryption stronger or weaker. The modes of operations that will be focused on are ECB, CBC, and CTR. Each of them will have the following:

- How they work
- Diagrams explaining the process
- Advantages & Disadvantages

Interactive sections showing the output of user inputted text, so the user can engage with the different modes of operation.

Module 4: Hashing Algorithms

Topics:

- What is a Hashing Algorithm
 - o Explaining hashing
- Strength of hashing
 - o Collision resistance, Preimage resistance
- Different types
 - o SHA1, MD5, SHA256
- When & where it's used
 - o I.e., Passwords, Files

Breakdown:

The core topic of module four is hashing, it will explain what a hashing algorithm is i.e., a one-way encryption. Explain the goal of hashing on how it should be irreversible. Visuals of how it operates so the process can be viewed.

What makes a hashing algorithm strong, i.e. it is both collision and preimage resistance, explaining what both of them are, and provide examples of both collision and preimage resistance.

Demonstrating different hashing algorithms, MD5, SHA1, and SHA256. Explaining how MD5 and SHA1 are no longer secure as they have vulnerabilities. Providing an interactive section where the user can use the different hashing algorithms on inputted text.

Supplying the users with information about where and when they may see a hashing algorithm in use, i.e. securing passwords, files for verification purposes, databases for integrity purposes, etc.

Module 5: Key Management

Topics:

- Importance of Key Management
 - o Explaining why it's important
- Key Generation
 - o Randomness needed
- Key Storage
 - o Different Methods of Storing Keys
- Key Life cycle diagram
 - o The Life of a Key

Breakdown:

The last module will purely focus on the importance and usage of a key. It will emphasize that the key is the main vulnerability of encryptions, and how it needs to be properly handled, generated, and stored.

Will describe the need to use pure randomness during its stage of generation, and how cryptographic keys need to be used. The different characteristics of a strong key, such as its length and randomness.

Different methods of storing keys such as key vaults, different hardware options, and software options, the advantages and disadvantages of each.

A dataflow-type diagram explaining the life of a key, including rotation revocation and expiration. The diagram will be from the key generation to its usage, to storage, rotation, revocation, and expiration.

Deliverables

The success of CipherCraft relies on the development and delivery of all the different functions and components required. To outline the objectives of CipherCraft they have been split into two main groups, core deliverables which are necessary for the functioning of CipherCraft. Non-core deliverables are functions that will enhance the platform. These deliverables put together will create the educational platform CipherCraft. For a timeline of development for each deliverable please see [Project Plan](#).

Development Core Deliverables

Account Management:

Account management, allows a user to create an account, be able to log in successfully with the correct credentials, and be prompted with an error message if the credentials are incorrect. While also providing the users the option to change their password if they have forgotten it.

This is a crucial function of the platform as without an account it will be difficult to track a user's progress and be able to correctly manage which modules they have access to. By ensuring that each user has an account it will allow for them to view their progress and improvements throughout the course.

To ensure that account management works correctly will depend on the use of a database. Which will contain all of the user's login details securely. The database will be used as a reference to ensure that the credentials are correct.

Testing will be used to ensure that the database is correctly constructed and linked to ensure that any difficulties that may arise are solved swiftly.

Interactive Learning:

Interactive learning is the area where the users of the platform will be able to engage with the website and learn from different inputs and outputs. They will be common and used throughout the encryption and decryption methods being taught.

The interactive sections will take inputs such as plaintext to be encrypted and display the ciphertext, and different keys so that the users can view the outputs, for decryption processes be able to click and enter different text to view didn't information.

As interactive learning deals with user input, the main concern is handling that input correctly so that malicious users do not tamper with the platform and destroy or deface the web page.

Testing will be done to ensure that user input is correctly handled and that malicious code cannot be executed through the input, as well as testing that the functionality of the interactive activities works correctly.

User Profile & Progress Tracking:

The user profile is where the user can go to continue the course where they left off view their progress and see how far they have come, and the results they got on each of the quizzes they took. A breakdown of each module and what the next topic is that they will learn.

This is a critical aspect of CipherCraft as it makes the platform unique from the rest, as it tracks the user's progress, improvements, results, and other information about their account.

The user profile has many dependencies such as the ability to create an account, ensuring that the progress of the course is tracked accurately and true, and that assessment results are correctly stored and visible to the user.

To test that the user profile and progress tracking is correctly implemented a test account will be created to ensure that all aspects of the profile work correctly and are displayed accurately.

Assessment System:

The assessment system consists the multiple-choice quizzes that are held after the completion of each module. The quizzes should use a random order of pre-described questions. The results of the quiz will determine if the user can progress to the next module or will have to repeat the quiz.

The assessment system is a major aspect of the platform as it allows the user to ensure themselves they are learning and progressing throughout the use of the course. It will also make sure that users are not progressing to topics too difficult for their level of knowledge.

The assessment system will only function correctly if the questions are provided in random order every time it is taken this way the users are not continuously clicking the correct answers each time and must read the questions and the optional answers.

Testing the randomness of the assessment system is the key aspect of this deliverable, running through the quiz multiple times will help make sure that the randomness is correctly working, and that the quiz functionality is also correctly implemented.

Material Visual & Written:

The material is how the users will primarily learn from the platform, using both written and visual to ensure that all aspects of learning are conveyed and not just focused on a certain method of learning. The material is a crucial component of CipherCraft as it is what makes the platform an educational teaching web application.

To make sure that the material used is acceptable for displaying and learning it shall be brought to different lecturers for a review and recommendations.

Graphical User Interface (GUI):

The GUI is where the user will interact with the platform, creating the layout, user interface elements and the overall design which will determine the level of engagement that the users will have when using the platform.

The GUI will be user-friendly meaning it will provide clear navigation methods, interactive elements and be aesthetically pleasing. The GUI will have a visual consistency meaning the color scheme will be the same throughout.

Admin Control Panel:

The admin control panel is where the admin can go to make necessary changes to the web page and its content. This provides a method of making sure any mistakes made can be altered and changed without having to scroll through the code.

The admin control panel is necessary as it provides for quick fixes to small mistakes made in the content or layout of the platform. This allows for fast changes without worrying about making more mistakes while going through the code.

The admin control panel will only be accessible to the admin login and no other logins. The admin will be a built-in account that has access to the different options for altering the platform and its content.

Testing for this will be crucial as being able to log in as admin should be hidden and difficult to do as it will provide options to alter the platform, making it a security threat. Testing that the functions for altering the platform also work correctly will have to be conducted to lengths.

Document Core Deliverables

Specification Document:

The specifications document will provide an outline for CipherCraft, detailing the different aspects of the web-based application project, including topics such as where the idea came from, the need for a project of this sort, who the target audience is, what the project requires, what technologies the project will contain, and a detailed plan on how to complete the project.

Research Document:

This is a document that will demonstrate all of the decisions made related to the project, from why certain technologies were chosen to the different methods of teaching. Any important aspect of the project will contain a research aspect, which will be documented in the research document.

Research Poster:

The research poster will consist of the key points found in the research document, displayed in a poster format. It will consist of visual and readable information, such as images, graphs, bullet-pointed findings, and any other information required. The research poster will convey a clear and concise way of understanding how and why CipherCraft came to exist.

Presentation:

The presentation to be given will display what CipherCraft is, so preparation for this must be completed such as creating a PowerPoint presentation that will display visually what the project is, and how much progress is being made.

Final Document:

This is to be completed after CipherCraft has come to completion, it will detail any problems and solutions, which aspects were completed and incomplete, the different learning curves, alternate approaches to this project, additional research if necessary, difficulties faced implementing aspects of the project, and any issues encountered with the tools.

Non-Core Deliverables

Lab Instructions:

The lab instructions are a set list of step-by-step instructions on how to implement different encryption methods, it would include code snippets with explanations of what the code is doing for those who are unfamiliar with programming, it may be difficult. A clear and concise explanation would be required.

It would be beneficial as it would allow the users to gain hands-on experience with implementing the different encryption methods, and allow them to become more familiar with programming different cryptography principles and best practices.

To test this I would provide the lab instructions to individuals both familiar and unfamiliar with programming and review how they managed the lab instructions and create changes when and where necessary.

Additional Educational Resources:

Providing a section where users can go and further their level of knowledge about cryptography. This would include an overview with links to different websites and platforms that contain more in-depth information and concepts around cryptography.

This would benefit the platform by providing a location for users who find the subject interesting to delve deeper into the topic.

User Feedback:

This would provide a section where users can make suggestions and ideas to help enhance the platform and provided feedback about any information that is incorrect or isn't very transparent. Allowing for the users to also take part in the construction of the platform.

This would be beneficial as it would allow for constructive criticism and for the users to feel a part of the CipherCraft community.

Gamification:

To make the platform more engaging the use of gamification could be used so that users feel as if they are working towards a goal or achievement while learning about the topic. The use of creating a leveling system and experience points to provide the feeling of progress. The use of badges for achievements would also be incorporated so that users can show off the awards.

The benefit of using a gamification approach is that it would attract goal-orientated people who would engage in trying to achieve all of the badges and achievements that would be associated with the platform.

To ensure that gamification works, setting up different achievements and badges would be necessary, and testing that they function correctly, I.e. a badge and or achievement for the completion of each module could be created and tested by completing each module.

Discussion Board:

The discussion board would be a place where users can go to discuss different topics related to cryptography and the course they are all taking, may it be for asking for help or providing help to others, the discussion board will be a public place for all users to communicate with each other.

It would allow users to create threads and discuss a topic, ask questions, obtain opinions and thoughts, etc. A discussion board would allow for a community to be built amongst the users of CipherCraft.

As the discussion board would take user input, it displays the ability for vulnerabilities in the project. Testing would be crucial to ensure that all vulnerabilities are mitigated.

Technologies

Languages: Python, HTML, CSS, JavaScript

The main language used to create CipherCraft is Python, which will manage the server-side data. The frontend interface will use HTML, CSS, and JavaScript. HTML will be the backbone of the web page creating the layout and structure. CSS is the programming language used to make websites aesthetically pleasing, giving them a professional and user-friendly design. JavaScript will be used for any front-end interactive sections that are needed.

Python:

Python is a high-level programming language, it supports both dynamic typing and binding, as well as code reuse with modules and packages. It primarily focuses on readability with the use of easy-to-learn syntax. The Python library is also massive, free, and open-source. (Python)

Although Python is a general-purpose programming language, it can also be used as a web development programming language with the use of frameworks. Frameworks are predefined packages that stand for the foundation and or structure of the website. Python is widely used to create websites due to the frameworks they provide. (Python2) (Tutorial)

I have chosen Python for the fact that it is easy to learn, and I already have a background using Python, it contains a wide library which is beneficial in the creation of this project. It provides ease of debugging as it displays exceptions as the errors are detected.

HTML:

Hyper Text Markup Language otherwise known as HTML, is a standard language when it comes to creating websites. Most if not all websites contain HTML. HTML is used to create the structure of a web page with the use of different tags, these elements are then used to inform the browser how the content should be displayed. (HTML)

The decision to use HTML for the production process of CipherCraft is due to the experience I have with the language and the benefits it provides such as allowing for methods to design the layout and structure of the web page with the use of different tags. These different elements allow for different visual effects such as lists, headings, links, etc.

CSS:

Cascading Style Sheets (CSS) is used in conjunction with HTML it provides a method of how and where the elements used in HTML will look and feel. CSS can be utilized within a stylesheet which can describe the layout and design of many different elements. (CSS)

CSS has been chosen to provide an aesthetically pleasing visual look to CipherCraft. As it works well with HTML it is the best decision to display a visually pleasing look to the website. My familiarity is also a contributing factor to the selection of CSS.

JavaScript:

JavaScript is a programming language that is used in many different sectors of programming from web development to gaming JavaScript has seen it all. When it comes to web development JavaScript provides a dynamic approach allowing for the addition of new elements as well as altering existing ones. It is primarily used to enhance a website by including interactive elements to the webpage. (JavaScript)

JavaScript will be beneficial to the development of CipherCraft as it provides methods to make the platform more engaging with the use of interactive methods. The knowledge I have of JavaScript is another reason for its inclusion in creating CipherCraft.

Framework: Flask, Django

Flask:

Offers simplicity and minimalism, a micro-framework, meaning it allows for the project developer to be more flexible with how they use the framework. Flask is lightweight and has a smaller codebase and fewer built-in features. The flexibility that Flask offers makes it a very enticing framework, as it allows for the freedom of choosing your own components and libraries, which is great when integrating. (Flask)

Django:

High-level framework that contains a wide range of built-in features and tools, these built-in features can help save time during the development stage. Django includes many common web development features, which is advantageous when needing to set up the platform swiftly. Django has a strong emphasis on security, making it good for websites that deal with sensitive data. The scalability of Django makes it suited for large web applications. (Django)

Tools: Visual Studio Code, XAMPP, GitHub

A suite of different tools has been chosen to enhance the development of CipherCraft. These tools will benefit both the production speed and technical needs that are required to ensure the development of CipherCraft is successful. Below you will see a detailed description of each tool and the decision process.

Visual Studio Code:

Visual Studio Code is a free lightweight yet powerful Integrated Development Environment (IDE). It has many different extensions available for many different programming languages. It supports languages such as Python, HTML, CSS, and JavaScript. (VSC)

My experience with Visual Studio Code is a key factor in my decision to make it my source code editor. The fact that Visual Studio Code also supports languages such as Python, HTML, CSS, and JavaScript is another factor that brought this decision to a conclusion.

XAMPP:

XAMPP stands for Cross-Platform, Apache, MySQL, PHP, Perl. It is a web server solution package that is free and open source. It allows for testing of web servers on a local host using Apache HTTP Server. It uses a control panel to determine which of its functions are currently running, with the use of a start and stop button. (XAMPP) (XAMPP2)

The decision to use XAMPP is due to previous experience, and its simplicity. The need to test CipherCraft is evident in the Gantt Chart (See [Project Plan](#)) and the best way to test is by using the Apache server available on XAMPP.

GitHub:

GitHub is a website that provides cloud-based storage for code, it is widely used by programmers as a method to manage and maintain their projects. It keeps track of any changes made to the code and allows for collaboration, making it easier to work in a team. (GitHub)

I have decided to use GitHub as it allows for storage and tracking of changes made to the source code. This will benefit the production by having backups of different times in the process of creating CipherCraft in case of unforeseen issues.

Database: MySQL, Docker

MySQL will be used to create a database that will store all user data, such as the login information, the user's progress, the quiz results, and any other necessary data. MySQL comes with XAMPP and can run through the control panel of XAMPP alongside the Apache server. Docker will be used to create a container for my database, as it will ensure isolation and help simplify database management.

MySQL:

MySQL is an extremely popular open-source database management system. It is used to store data in a structured form. It can store many different forms of data such as numbers, characters, strings, and even dates. MySQL can also link different databases together so the information related to a certain piece of data can be stored separately. (MySQL) (MySQL2)

The decision to use MySQL was clear from the start as it provides a structured method of storing data, which is required for the success of CipherCraft. I also have background and experience using MySQL database systems.

Docker:

Docker is a platform used for developing and running applications. It allows for the separation of applications and infrastructure so software can be delivered quickly. It uses isolated environments called containers, you may have multiple containers running at the same time. (Docker)

I have decided to use docker in conjunction with my database as it allows for isolation and will prevent any possible conflicts that may arise. I also have experience using docker to contain databases that worked well with XAMPP.

Interface Design

The image below is a flowchart of how the user may interact with the platform. The flowchart was created using Draw.io.

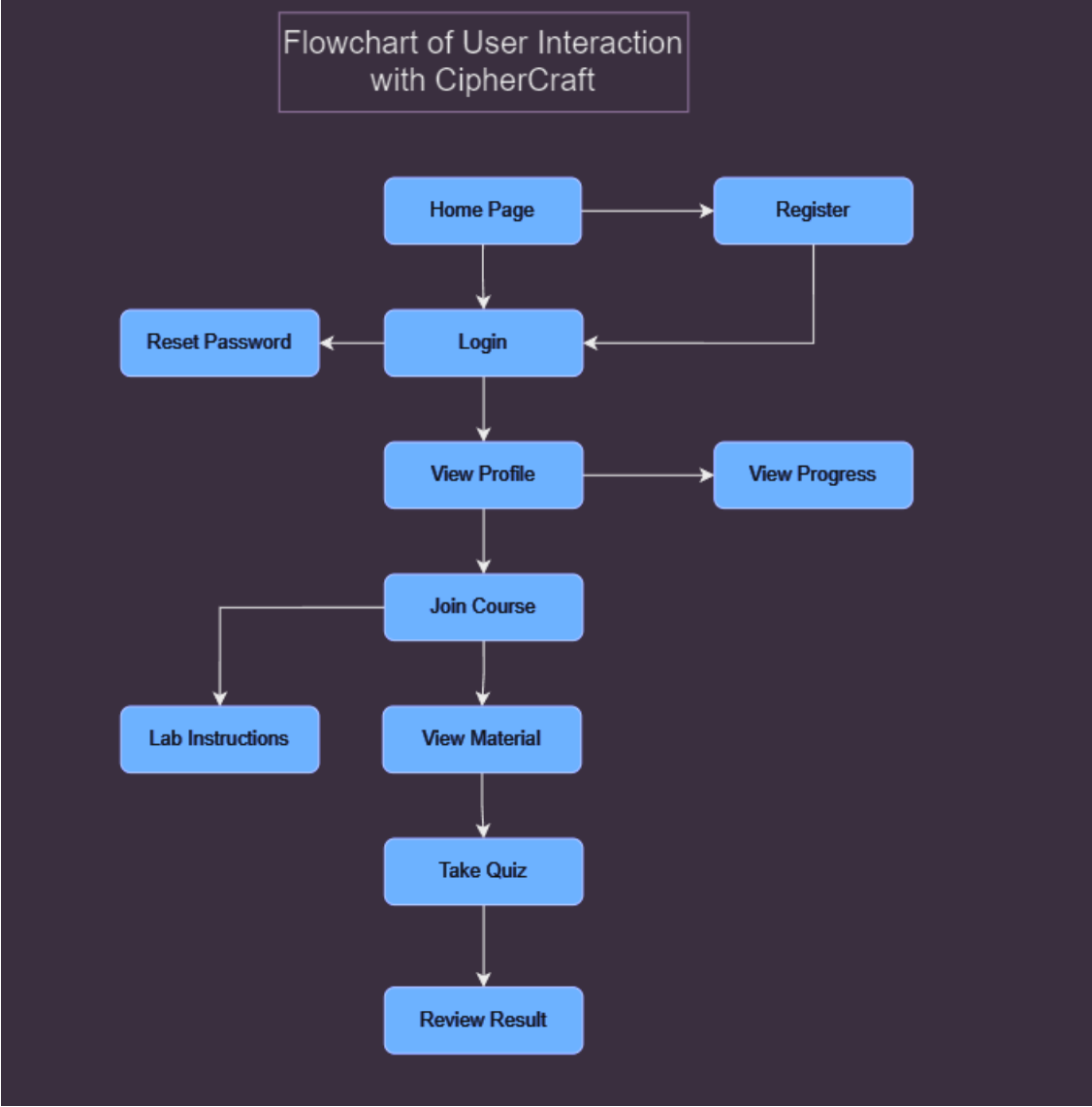


Figure 2:Flowchart Interaction

Login / Sign up Page

As CipherCraft is for everyone that is interested in delving into the world of cryptography, there must be a method for signing up and logging into the web page. The design is simple and easy for users to understand.

The sign up page allows for a user to create an account by entering the following information:

- Username : So they have a unique identifier
- Email : To verify that the individual is a person and to allow for emails to be sent directly to them
- Password : As a safe measure for being able to access their information
- Confirm Password : To make sure that they have entered the password correctly

Example Layout:

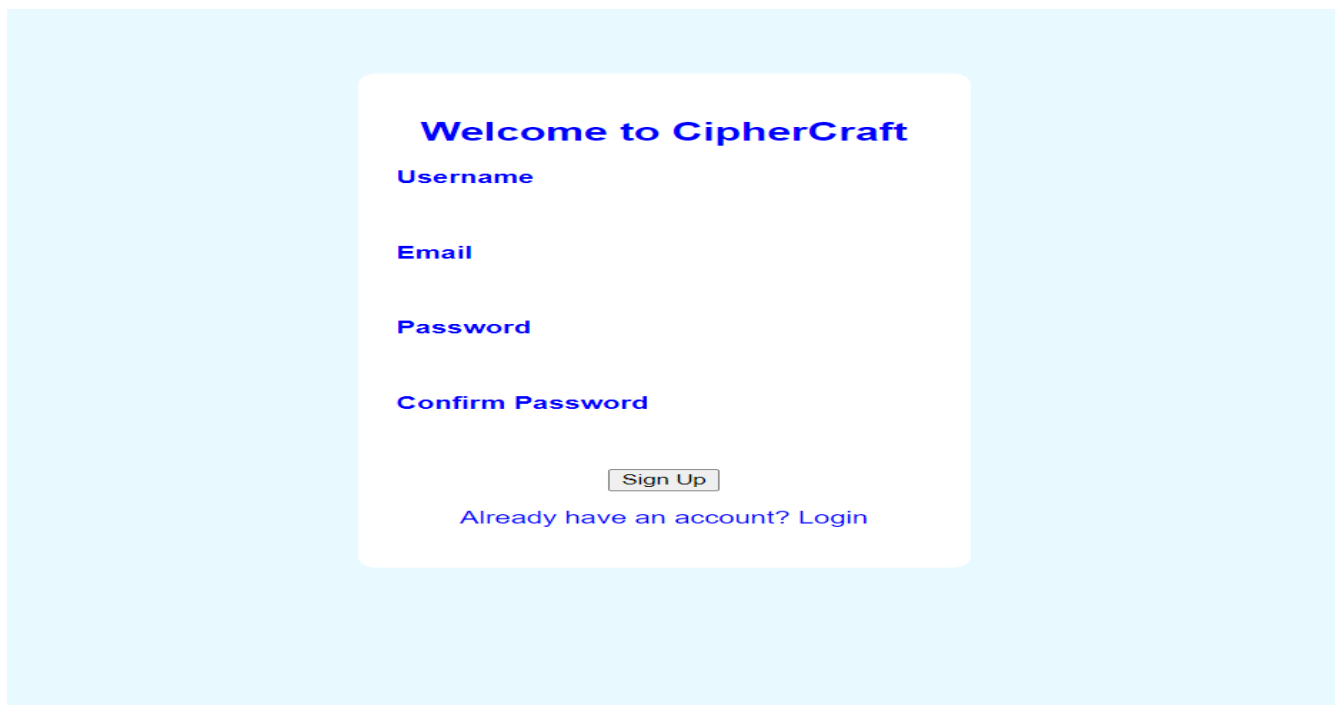


Figure 3: Sign Up Page

The login page follows the same style of the Sign up page, but requests the users username and password credentials so it can determine that the user is who they say they are and not just another individual. It also contains a method of resetting the password in cases where the user has forgotten it.

Example Layout:

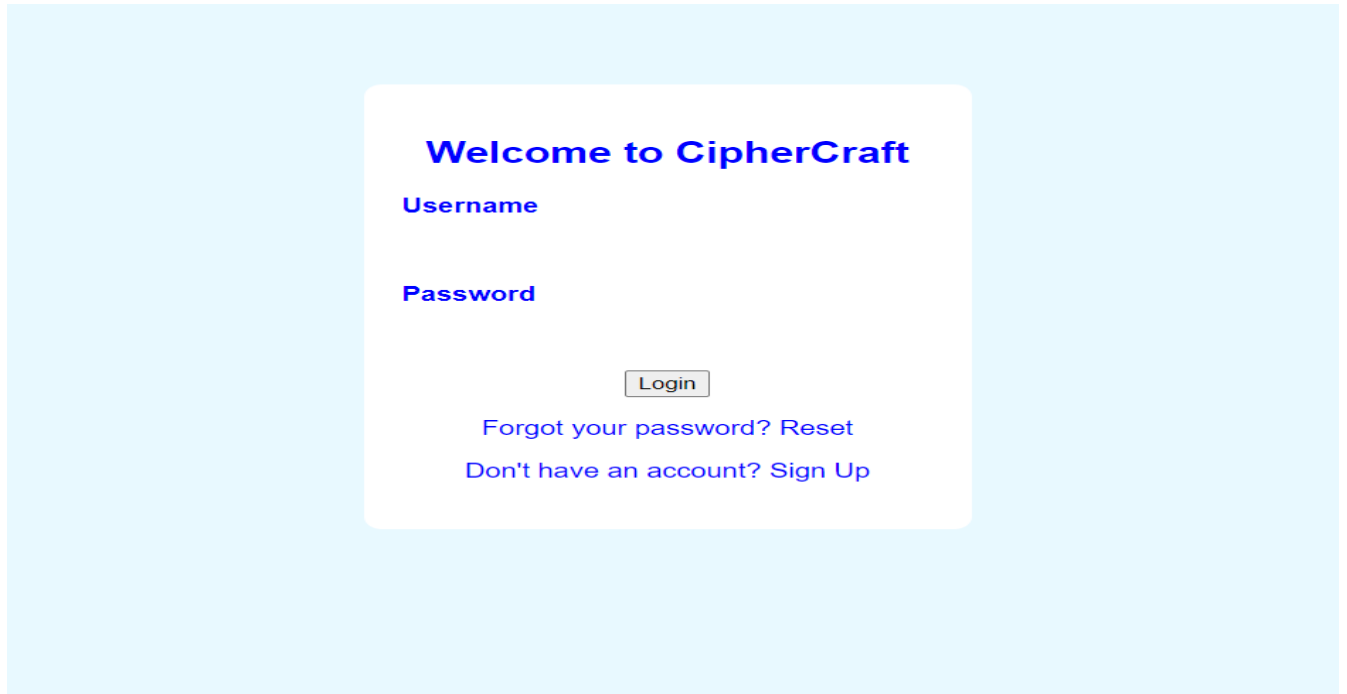


Figure 4: Login Page

Dashboard / Main Page

The dashboard of CipherCraft, is the main home page that everyone will be sent to, here they can discover and traverse CipherCraft. It will contain information about the course, be able to start the course, continue the course where they have left off. Learn more about cryptography from additional resources, and discover why cryptography is important.

Example Layout:



Figure 5:Dashboard

Course Page

The course page represents the content that will be taught to the users of CipherCraft. It's layout is simple and user friendly, it states the module name, under it shall present all of the content required for that modules topic. With a button to allow the students to move on to the next section.

Example Layout:

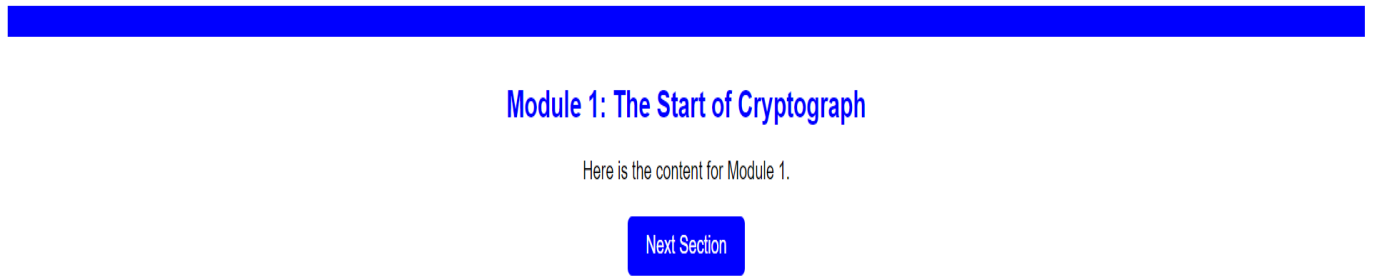


Figure 6:Course Page

Quiz Page

The quiz page is where the user will determine if they have learned enough to progress to the next stage. They will be presented with a question, and multiple choice answers where they will select which of the answers they believed to be correct. The page will contain two buttons a 'Previous'

and 'Next' these buttons will allow the user to move between questions in case they are unsure of the answer they can traverse them. When a user selects an answer it will be highlighted so they know which one they have selected.

Example Layout:

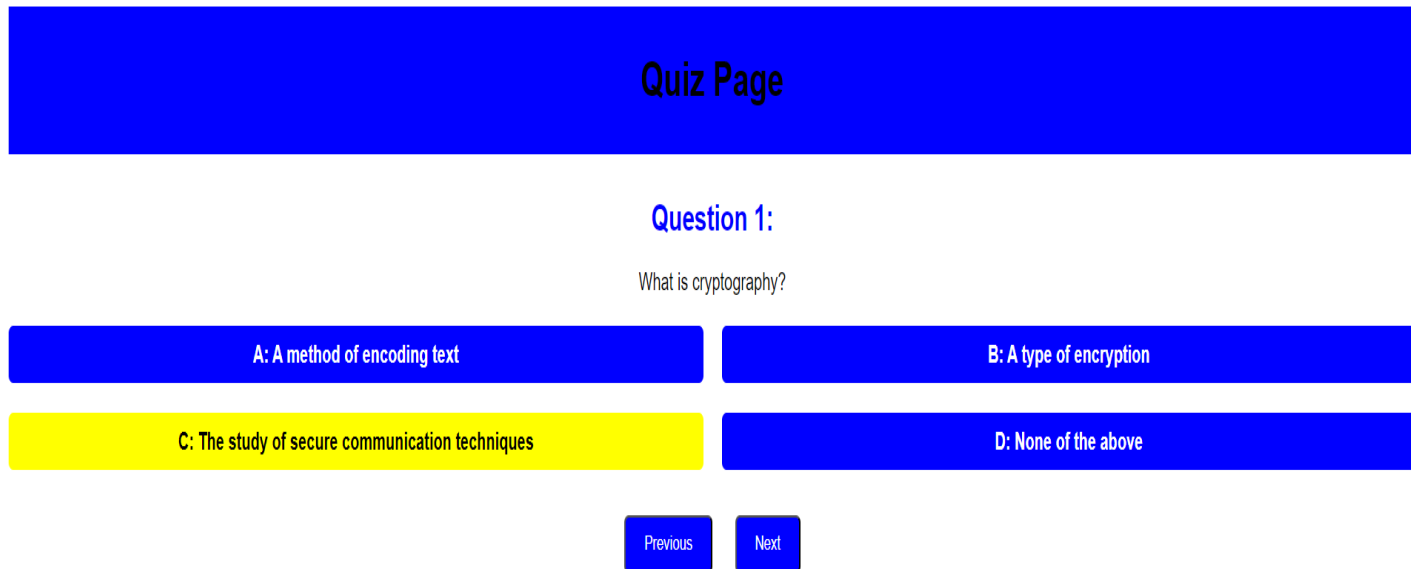
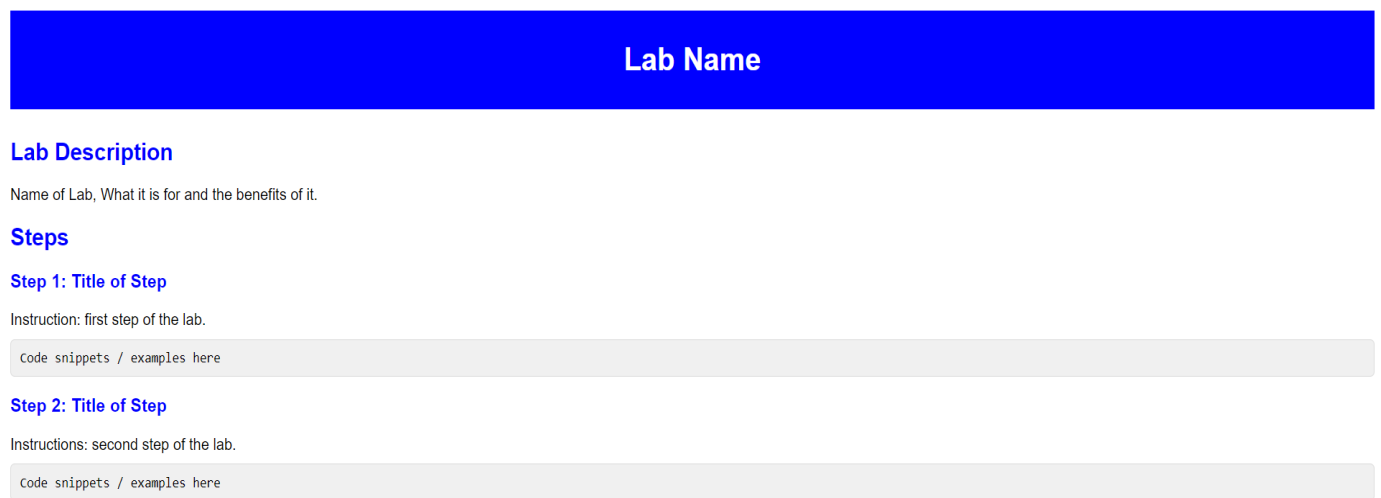


Figure 7: Quiz Page

Lab Page

The lab page will have a set of instructions detailing how to complete the lab. It will contain a name of the lab, a description of what the user is going to accomplish during the lab, and the benefits of being able to utilize and implement these methods.

Example Layout:



The image shows a wireframe for a lab page. At the top is a solid blue horizontal bar with the text "Lab Name" centered in white. Below this bar is the section "Lab Description" in blue, followed by a line of placeholder text: "Name of Lab, What it is for and the benefits of it." The next section is "Steps" in blue. Under "Steps", there are two identical step entries. Each entry starts with a blue heading "Step 1: Title of Step" (or "Step 2: Title of Step" for the second), followed by a line of placeholder text: "Instruction: first step of the lab." (or "Instructions: second step of the lab."). Below each instruction is a light gray rounded rectangular box containing the placeholder text "Code snippets / examples here".

Figure 8: Lab Page

Profile Page

The profile page is where the user can go to learn more about their progress, and achievements. The profile page will display the users information, such as their Username, Email, and Level. The progress they have made on the modules, with their quiz results, and the different achievement that they have gained throughout the course.

Example Layout:

The image shows a user profile page layout. It features a blue header bar at the top. Below the header, there is a white rounded rectangle containing the following information:

- User Information**
 - Username:** JohnDoe123
 - Email:** johndoe@example.com
 - Level:** Intermediate

Below the white box, on a light gray background, are three sections:

- Module Progress**
 - Module 1: 30%
 - Module 2: 60%
 - Module 3: 15%
- Quiz Scores**
 - Module 1 Quiz: 85%
 - Module 2 Quiz: 70%
 - Module 3 Quiz: 90%
- Achievements**
 - Module 1 Completion
 - Module 2 Completion

Figure 9: Profile Page

Metrics

The following will determine the success of CipherCraft. Each metric will be able to determine the usability, feasibility, functionality, and performance of CipherCraft.

1. Can CipherCraft operate on any browser i.e can properly function on Google, Firefox, Microsoft edge etc.
2. The a user is able to create an account and gain access to the teaching materials.
3. That the material used is correct and true, usable in the real world.
4. That users are able to engage with the platform, during the teaching moments.
5. That all quiz questions are randomly displayed.
6. That the user can visually see the progress they made with each module
7. User feedback, allow for testing of the platform from a group of randomly selected individuals and have them rate the platform on different topics, such as:
 - a. The usability of the platform, was it easy to navigate the platform.
 - b. Was the design of the platform user friendly.
 - c. Did you enjoy taking the course.
 - d. Would you recommend it to someone wanting to learn about cryptography.

FURPS

FURPS is an acronym that stands for Functionality, Usability, Reliability, Performance, and Supportability. It is used to collect a complete set of project requirements without overlooking any of the essential non-functional requirements and expectations of a customer and end-user. (Gehtsoft)

Functionality:

The functionality aspect is critical as it relates to the core purpose of CipherCraft. It contains the main functions and how they are used to achieve the purpose. Below is a list of the purposes and functions of CipherCraft.

- Providing a clear and organized curriculum with different modules to teach the basics of cryptography.
- Allowing users to create an account, log in, join the course, view course material, and be able to view their progress.
- Using interactive learning components for hands-on learning.
- Allowing administrators to manage the platform.

Usability:

Usability refers to how usable the platform is, does it provides a navigation system, is it difficult to locate certain sectors of the platform. The usability of the platform must be present so the users can have an enjoyable experience using the platform. Below is a list of components used to ensure the usability of the platform.

- The graphical user interface is user-friendly.
- User profiles and progress tracking for monitoring and navigation.
- Interactive learning for engaging learning experiences.

Reliability:

The reliability of any platform is essential as it ensures that the information provided is up-to-date and trustworthy. Below is a list to ensure that the reliability of CipherCraft is visible.

- Providing methods for administrators to make updates and changes when necessary through the admin control panel.
- Using assessments to evaluate user's knowledge after completing the modules.
- Allowing users to interact with the use of a discussion board.

Performance:

Performance relates to the level of engagement and responsiveness of the users when participating in the course. Below is a list of methods used to support the performance of CipherCraft.

- The use of randomly ordered questions in the assessment.
- Gamification of the platform.

Supportability:

Supportability is summed up as future improvements and maintenance of the platform. Below is a list of the features to ensure the supportability of CipherCraft.

- The admin control panel allows for changes and updates to be made.
- Discussion board and feedback from the users.
- Supplying additional resource options to patrons of CipherCraft.

Project Plan

Project libre was used to create a Gantt chart(See below), which illustrates a plan of action to complete the project swiftly. It is broken down between Documentation and Development requirements, both headings each contain the deliverables required. A key is provided for ease of reading.

Key	
Blue bar	Non-Critical tasks

Red bar	Critical tasks
Thick black bar	Task inside a heading
Small black bar	Links between tasks



Figure 10: Gantt Chart 1/2

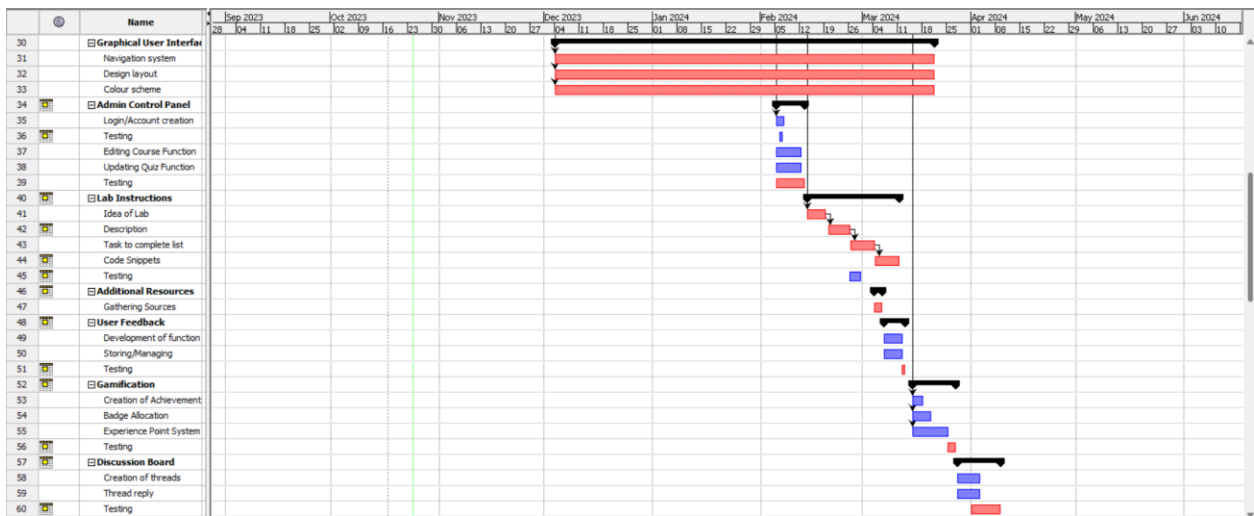


Figure 11:Gantt Chart 2/2

References

(n.d.). Retrieved from <https://gehtsoftusa.com/blog/create-better-backlog-and-engage-the-development-team-with-furps/#:~:text=It%20stands%20for%20Functionality%2C%20Usability,a%20customer%20and%20end%2Dusers.>

(n.d.). Retrieved from <https://www.python.org/doc/essays/blurb/>

(n.d.). Retrieved from <https://www.python.org/doc/essays/blurb/>

- (n.d.). Retrieved from https://www.w3schools.com/html/html_intro.asp
- (n.d.). Retrieved from <https://www.tutorialspoint.com/can-we-build-a-website-from-python#:~:text=Python%20provides%20a%20lot%20of,one%20of%20its%20primary%20features.>
- (n.d.). Retrieved from https://www.w3schools.com/css/css_intro.asp
- (n.d.). Retrieved from <https://www.computerscience.org/bootcamps/guides/javascript-uses/#popular>
- (n.d.). Retrieved from <https://kinsta.com/blog/flask-vs-django/#:~:text=Flask%20tends%20to%20be%20simpler,%2C%20demands%2C%20and%20existing%20requirements.>
- (n.d.). Retrieved from <https://kinsta.com/blog/flask-vs-django/#:~:text=Flask%20tends%20to%20be%20simpler,%2C%20demands%2C%20and%20existing%20requirements.>
- (n.d.). Retrieved from <https://code.visualstudio.com/docs>
- (n.d.). Retrieved from <https://code.visualstudio.com/docs>
- (n.d.). Retrieved from <https://www.educba.com/what-is-xampp/>
- (n.d.). Retrieved from <https://www.simplilearn.com/tutorials/php-tutorial/php-using-xampp#:~:text=on%20your%20PC.-,What%20is%20XAMPP%3F,on%20a%20local%20host%20webserver.>
- (n.d.). Retrieved from <https://kinsta.com/knowledgebase/what-is-github/>
- (n.d.). Retrieved from <https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html>
- (n.d.). Retrieved from <https://www.oracle.com/mysql/what-is-mysql/>
- (n.d.). Retrieved from <https://docs.docker.com/get-started/overview/>
- (n.d.). Retrieved from <https://blogs.ucl.ac.uk/infosec/2017/03/12/applications-of-cryptography/>
- (n.d.). Retrieved from <https://www.cryptool.org/en/>
- (n.d.). Retrieved from <https://cryptopals.com/>