SOFTWARE REQUIREMENTS SPECIFICATION

for

Cipher Craft

Version 1.0

Prepared by : 1. Kunal Demla (102003088)
2. Gaurav Pahwa (102003087)
3. Ramneet Singh (102003071)
4. Gurkirat Singh (102003085)

Submitted to : Ms. Kanupriya

August 29, 2022

Contents

1 Introduction

1.1 Purpose

The purpose of this document is to build a text, image and file encryption system to achieve a secure and easy transfer of the same over the network and to make the users aware of importance of encryption and their working principles.

1.2 Document Conventions

The Abbreviations used in this document are:

- PoTD - Problem of the Day
- CoTM - Cipher of the Month
- ToH - Tower of Hanoi

1.3 Intended Audience and Reading Suggestions

This project is a prototype for a powerful and multipurpose encryption system and it is for study purpose only. This has been implemented under the guidance of college professors. This project is useful for the security enthusiasts and users who are cautious about their privacy.

1.4 Product Scope

The purpose of the Cipher Craft encryption system is to ease text, image and file encryption and to create a user friendly web application for security enthusiasts and users trying to secure their data. The system is based on various algorithms which are used to encrypt and secure data. We will have a server supporting various encryption and services. Above all, we hope to provide a comfortable user experience along with the best security available.

1.5 References

- Dcode.fr
- Boxentriq

- CyberChef

2 Overall Description

2.1 Product Perspective

"Cipher Craft" is a powerful, user-friendly and educative tool for encryption and security purposes
A web-application that provides the following categories of services:

- **Cryptography**
  Cryptography is defined as the process of converting useful information into an unrecognizable form to protect it from unauthorized access.
- **Steganography**
  Steganography is the technique of hiding secret data within an ordinary or non-secret file in order to avoid detection; the secret data is then extracted at its destination.
- **Games and Solvers**
  This includes some common tools to solve famous games and problems like Sudoku and Tower of Hanoi.
- **File Encryption**
  File encryption is a way of encoding files, including the sensitive data they contain, in order to send them securely. The encoding prevents unauthorized access and tampering by malicious actors. It keeps a file from being read by anyone except the person or people for whom it was intended.

2.2 Product Functions

The major features of Cipher Craft are as shown in the below Wireframe of the web application: (refer Fig 2.1)
The product should be able to perform the following operations:

- It must be able to Encrypt and Decrypt the data provided by the users.
- It must be able to give optimal and fast solutions to the problem/puzzle provided by the users.
- It must be able to authenticate and login the valid users.
- It must showcase the underlying principles and workings of the encryption algorithms.

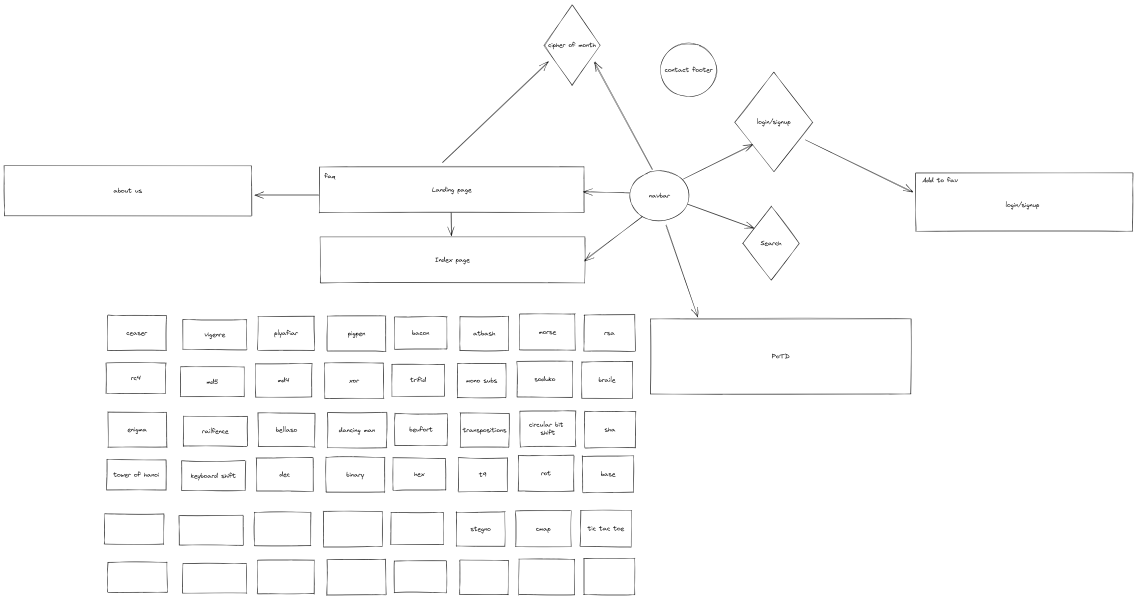

Figure 2.1: Plan

- It shall also provide a user support and help community to the users. (Implemented using Discord server/bots)

2.3 User Classes and Characteristics

"Cipher Craft" has basically 3 types of users.

- Admins/Developers
- General Users
  - Authenticated Users
  - Anonymous Users

General Users has 2 types - Authenticated Users shall have access to Puzzle of the Day, Cipher of the Month and a higher file upload size limit, while Anonymous Users not having the same privileges.
While everyone having an open access to all other kinds of encryptions and solvers available on the web-app with no privilege differences.
Along with the administrations having the following privileges:

- Add/Delete a Cipher.
- Add/Delete a Solver.
- Add/Delete Puzzles.

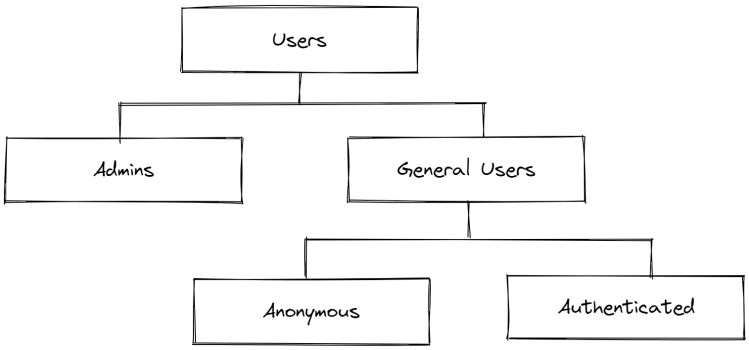

Figure 2.2: Types of Users

- Update Cipher of the Month.
- Add/Delete a User.
- Moderate the Help/Support Community.

2.4 Operating Environment

The website will be operate in any Operating Environment - Mac, Windows, Linux, iOS 9+, Android 4.4+ etc.
Using browsers such as - Chrome 45+, Firefox 38+, Opera 30+, Internet Explorer 10+, Edge 12+, Safari 9+ etc.

2.5 Design and Implementation Constraints

Design shall be made using wire-framing on Excalidraw and Front-end Design on Figma. For implementation of the software, we shall use Bootstrap for front-end while using Django for developing the back-end and SQLite as our database.

2.6 User Documentation

The Web-app shall provide:

1. An FAQ section about the web app.
2. A help/contact us/bug report section.
3. A dedicated Discord Server for exposure to our Community and Feedback.
4. A simple, easy to understand interface.
5. Every Solver/Cipher page includes explanation for the underlying Algorithm.

2.7 Assumptions and Dependencies

The following Assumptions and Dependencies have been kept in mind for the web app:

- The user has a Basic sense of how and what cipher, the user needs to use.
- The user has a system which can support the latest version of Bootstrap used.
- The server can support the latest version of Django used.
- The server has powerful enough computation limits to support the working and calculations.
- The services used such as Bootstrap, Django and any other reference/iframe remain and continue to provide their services.

3 External Interface Requirements

3.1 User Interfaces

The User interface shall comprise of the following: (Refer Figure 3.1)

- Screen Layout Constrains: 12 Column Grid Design (Using Bootstrap)
- Fonts Used:
  - Headings : Himagsikan
  - Sub-headings : Satisfy
  - Paragraph : NanumMyeongjo
- Colors Used:
  - Background : #DFF1AC
  - Headings : #023D26, #046E3E (Gradient)
  - Subheadings and Paragraphs : #191A19
  - Navbar : #254A25 - #2AAF2A (Linear Gradient at 90.27deg)
- Functions that appear on every screen are:
  - Navbar
  - Help
  - Contact Us
  - Share
  - Search Bar
- Shortcuts:
  - Shift + Enter : Executes the current block

3.2 Hardware Interfaces

The following list presents the Hardware interface requirements:

- The product requires very limited graphics usage.
- The interaction requires just a simple keyboard for taking the user input.

- A simple mouse/keyboard can be used to navigate the website.
- The product does not require usage of speaker/microphone, web-cam or animation and graphics.

3.3 Software Interfaces

The Software Interfaces used are:

- SQLite for Database.
- Django for Backend.
- Bootstrap for Frontend.

The requirements for usage of the application are:

- Any Operating Environment - Mac, Windows, Linux, iOS 9+, Android 4.4+ etc.
- Supporting browsers such as - Chrome 45+, Firefox 38+, Opera 30+, Internet Explorer 10+, Edge 12+, Safari 9+ etc.

3.4 Communications Interfaces

The requirements associated with communications functions required by this product are:

- Network server communications protocol used shall be HTTP/HTTPS using port 80/443 on the server.

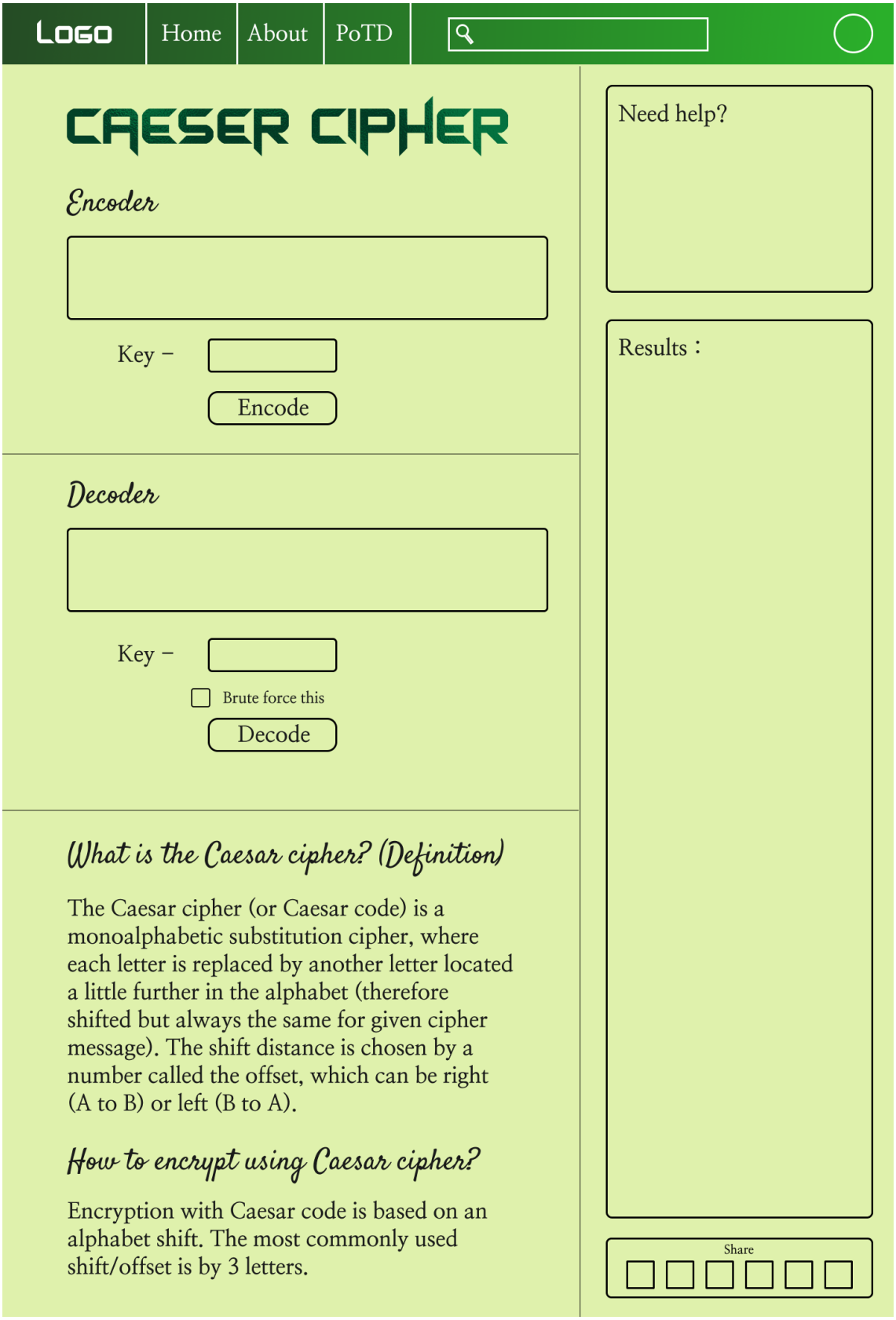

Figure 3.1: UI/UX

4 System Features

"Cipher Craft" is an Encrypting/Decrypting web software. So the main art of this product is to Encrypt, decyrpt and solve problems while distributing the knowledge of the working principles. "Cipher Craft" has features that are main and also some are sub. But all the feature is necessary for this software.

4.1 Login/Sign Up

Users can Login or Sign Up using email and password as the credentials. This gives access to PoTD, CoTM and larger file upload limits, along with an option to add ciphers to favorite.

4.2 Games and Solvers

- Tower of Hanoi Solver
- Soduko Solver
- Anagram Generator

4.3 Modern Cryptography

- Circular Bit Shift
- Deffi Hellman
- MD4 Hash
- MD5 Hash
- RC4
- RSA
- SHA1
- SHA256
- SHA512
- XOR

4.4 Poly-Alphabetic Cipher

- Alberi Cipher
- Beaufort Cipher
- Bellaso Cipher
- Trifid Cipher
- Vigenere Cipher

4.5 Transposition Cipher

- Caeser Box
- Column Transposition
- Double Transposition
- Railfence
- Scytale

4.6 Substitution Cipher

- Dorabella
- Pigpen
- Dancing men
- Hexahue
- Atbash
- Bacon
- Caeser
- Enigma
- Mono Alphabetic Substitution
- ROT47
- T9
- Semaphore

4.7 Polygrammic Cipher

- Bifid Cipher
- MultiTap SMS
- Playfair

4.8 Cryptography (Other/unclassified)

- Base64
- Base32
- Base10
- Hexadecimal
- Binary

4.9 Image Encryption

- PNG Chunks
- Henon-Arnold Chaotic Map Encryption

4.10 Steganography

- Exif Data
- Low Contrast
- Outguess
- Steghide

4.11 File Compression

- Tar
- Zip

4.12 File Encryption

- RSA
- AES
- DES

4.13 CoTM and PoTD

An exclusive **Cipher of the Month** made by developers for the Registered Users, Updated Monthly.
An exclusive **Problem of the Day** made by developers for the Registered Users, Updated Daily.

4.14 Search Bar

An efficient feature to search your required cipher from all the available ones quickly.

5 Other Nonfunctional Requirements

5.1 Performance Requirements

The results provided shall be accurate for all possible cases and the process should be done in minimum amount of time possible.
The compressions should be lossless, fast and considerably compressed in size compared to the original size.
The Web-app should be fast, responsive and easy to use.

5.2 Safety Requirements

The web-app and the company shall not be held responsible for any loss in data or usage of the app for any illegal or harmful purposes.
The company does not support or promote any illegal or inhumane activities.

5.3 Security Requirements

- The data should be sent in encrypted form from client to server.
- The passwords should be stored in hashed format with timestamps used as salt.
- No personal data / files uploaded should be accessible to developers or admins in any possible scenarios.

5.4 Software Quality Attributes

Adaptability, availability, correctness, flexibility, interoperability, maintainability, portability, reliability, reusability, robustness, testability, and usability shall all be enforced properly.
Logical, database and UI test is also required.

5.5 Business Rules

No business, only social service.
The web application is only for study purposes and shall be open source.
If needed, the costs for maintenance and hosting shall be gained using non pop up advertisements or via donations/charity.

6 Other Requirements

- About Us page
- Discord Support Server Community
- FAQs Page
- Contact Us/Support us sections