h./

Report – Cryptography

Team no. 30

99005720- Harsh Doshi

99005744- Chennupati geethika NA

99005725- Sai Vamsi Krishna Kadiyala

99005710- Ankit Duhan

99005757- P Heam Kumar

99005740- Harshit

99005754- Vismaya K

99005743-Shivani Yadawar

99005709- Mohammed Salih TS

99005728- Nikita Ramratan Hatwar

99005753- GopuRaman



Version Number:

Team Members :

Team No:

Module: Model Based System Engineering

Individual Contribution

|  |  |  |
| --- | --- | --- |
| **Ps no.** | **Name** | **Contribution** |
| 99005720 | Harsh Doshi | Test plan and workflow |
| 99005744 | Chennupati geethika NA | Requirements |
| 99005725 | Sai vamshi Krishna Kadiyala | Images and vedio |
| 99005710 | Ankit Duhan | Implementation |
| 99005757 | P Heam Kumar | workflow |
| 99005740 | Harshit | Implementation |
| 99005754 | Vismaya K | Report |
| 99005743 | Shivani Yadawar | Report |
| 99005709 | Mohammed Salih Ts | Workflow |
| 99005728 | Nikita Ramratan Hatwar | Design |
| 99005753 | GopuRaman | Design |

# 

**Table of contents:**

1. Individual contribution ----------------------------------------------------------------------------------------------------- 2
2. Introduction ------------------------------------------------------------------------------------------------------------------- 4
3. Requirements------------------------------------------------------------------------------------------------------------------4

3.1 Research ------------------------------------------------------------------------------------------------------------------------4

3.2 Target Audience ---------------------------------------------------------------------------------------------------------------5

3.3 Defining our System ----------------------------------------------------------------------------------------------------------5

3.4 Swot Analysis -------------------------------------------------------------------------------------------------------------------6

3.5 4W’s and 1H’s -------------------------------------------------------------------------------------------------------------------7

3.6 High Level Requirement ------------------------------------------------------------------------------------------------------8

3.7 Low level requirement --------------------------------------------------------------------------------------------------------9

4. Design -------------------------------------------------------------------------------------------------------------------------------10

4.1 Activity Diagram ----------------------------------------------------------------------------------------------------------------10

4.2 Block Diagram --------------------------------------------------------------------------------------------------------------------10

4.3 Level 0 DFD Encryption --------------------------------------------------------------------------------------------------------11

4.4 Level 1 DFD Encryption ---------------------------------------------------------------------------------------------------------11

4.5 Level 2 DFD Encryption ---------------------------------------------------------------------------------------------------------12

4.6 Sequence Diagram ---------------------------------------------------------------------------------------------------------------12

4.7 State chart Diagram --------------------------------------------------------------------------------------------------------------13

4.8 Usecase Diagram -----------------------------------------------------------------------------------------------------------------14

4.9 System outline Diagram --------------------------------------------------------------------------------------------------------15

5 Test Plan ------------------------------------------------------------------------------------------------------------------------------16

5.1 Low Level Test plan --------------------------------------------------------------------------------------------------------------16

6 Output Images ----------------------------------------------------------------------------------------------------------------------17

**Introduction**

The aim of this application is to throw light on the basics of Cryptography and Learn & Practice basic Encryption and Decryption through substitution techniques. Many Cyber Security courses expect students to have an understanding of essential concepts underlying Cryptographic system. The application covers five substitution techniques: Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher and Polyalphabetic Cipher.

1.Caesar cipher: It is a type of substitution cipher in which each letter in the plain text is replaced by a letter some fixed number of positions down the alphabet.

2. Monoalphabetic cipher: A monoalphabetic cipher is any cipher in which the letters of the plaintext are mapped to ciphertext letters based on a single alphabetic key.

3. Playfair cipher: It is a written code or symmetric encryption technique that was the first substitution cipher used for the encryption of data.

4. Hill cipher: The hill cipher technique uses a square matrix as the key used to encrypt and decrypt.

5. Polyalphabetic cipher: This is based on substitution using multiple substitution alphabets at different points in the encryption process.

**Requirement**

**Research**

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. cyber security is of absolute importance to today’s world and more people are starting to show interest in this field. While today’s cyber security systems have come a long way and evolved to combat modern problems, it is always beneficial to go back to the beginning and start from the basics. Many courses either move to advanced concepts swiftly after briefing the basics or indulge in too much detail which is exhausting for a beginner. Features of proposed application:

1. Concise Information: Every topic will consist of an introduction, the concept of encryption and decryption and the formulae used.

2. Practice: The user is prompted a set of questions which enables to check their understanding

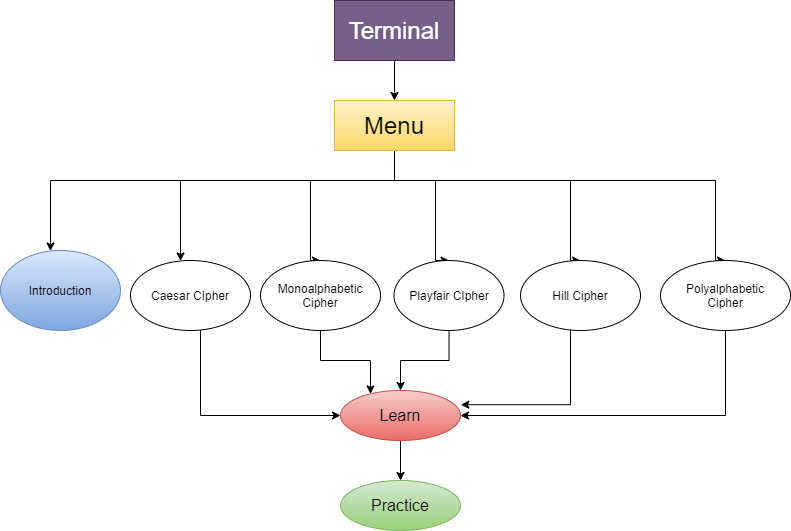
**Target Audience**

1. Computer Science (or related) Students/Faculties

2. Cryptography Enthusiasts

3. Beginners to Cyber Security

**Defining Our System**



The application provides the following options on entering

1. Introduction
2. Caesar Cipher
3. Monoalphabetic Cipher
4. Playfair Cipher
5. Hill Cipher
6. Polyalphabetic Cipher

**Swot Analysis**



**4W's and 1'H**

## **Who:**

This application aims to reach out to

1. Computer Science (or related) Students/Faculties
2. Cryptography Enthusiasts
3. Beginners to Cyber Security

## **What:**

The application aims for users to learn and practice basic encryption or decryption techniques. The application aims to be concise and apt for beginners in Cryptography. The application is built with C programming language and Make.

**When:**

Over the past few years, Cyber Security has gained momentum, Briefing about the basics of Cryptography is of utmost importance.

## **Where:**

This application can be utilised globally on an online platform.

## **How:**

By creating concise and apt modules along with simultaneous practice questions, the application aims to reduce exhaustion in learners and increases engagement.

# Detail requirements

## **High Level Requirements:**

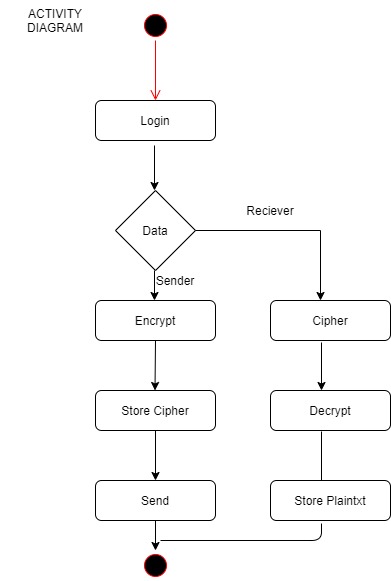
|  |  |  |
| --- | --- | --- |
| **ID** | **Description** | **Status (Implemented/Future)** |
| HR01 | User shall be able to choose what topic to explore | Implemented |
| HR02 | User shall be able to view and learn each topic | Implemented for one choice |
| HR03 | User shall be able to practice given questions for each topic | Implemented for one choice |
| HR04 | User shall be able to verify their answers for practice questions | Implemented for one choice |
| HR05 | System should be able to run smoothly with any given user input | Future |

## **Low level Requirements:**

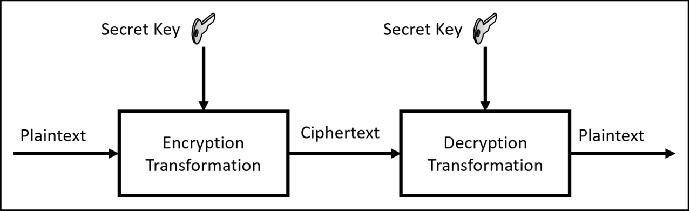
|  |  |  |
| --- | --- | --- |
| **ID** | **Description** | **Status (Implemented/Future)** |
| LR01 | User shall be able to choose topic in one of 6 ways from the Home page 1) Introduction 2) Caesar Cipher 3) Monoalphabetic Cipher 4) Playfair Cipher 5) Hill Cipher 6) Polyalphabteic Cipher | Implemented |
| LR02 | User shall be redirected to a new page containing Information depending on the choice of topic | Implemented for one choice |
| LR03 | User shall be able to choose to Practice or go to Home page | Future |
| LR04 | For every question user is prompted to enter a valid answer which is sent for verification | Implemented |
| LR05 | User shall be displayed error if entered input consists of characters except alphabet characters and space | Implemented |
| LR06 | User shall be able to receive a result of Correct/Incorrect for every answer to the Practice Question | Implemented |
| LR07 | User shall be able to choose to retry the Practice Questions for that topic or go back to Home page. | Future |

**Design**

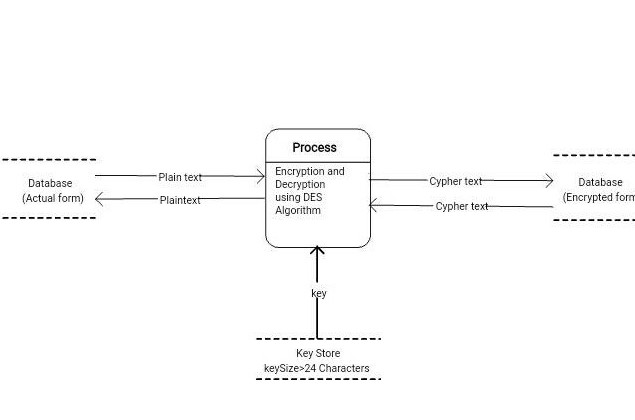
1. **Activity Diagram**



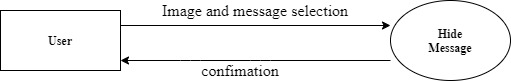
1. **Block Diagram**

****

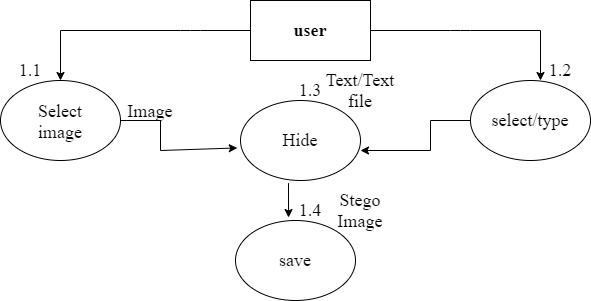
1. **Level 0 DFD Encryption Diagram**



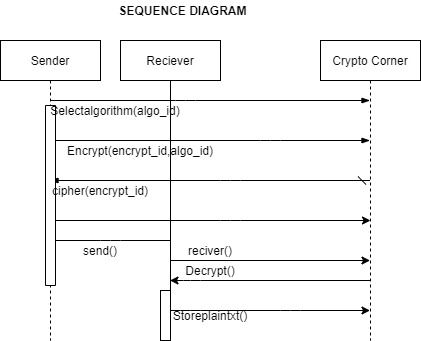
1. **Level 1 DFD Encryption Diagram**

****

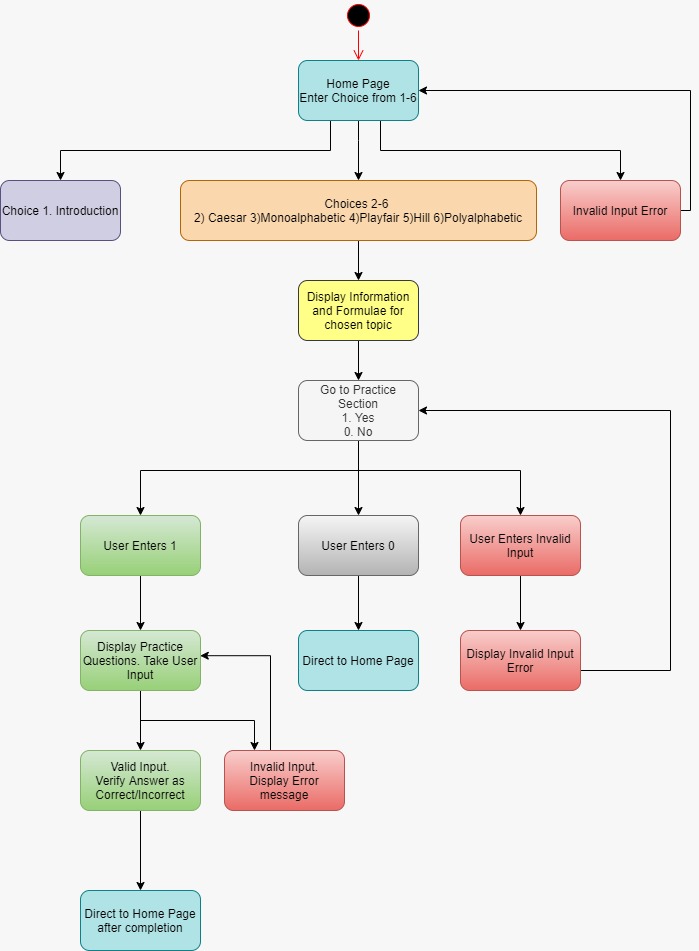
1. **Level 2 DFD Encryption Diagram**

****

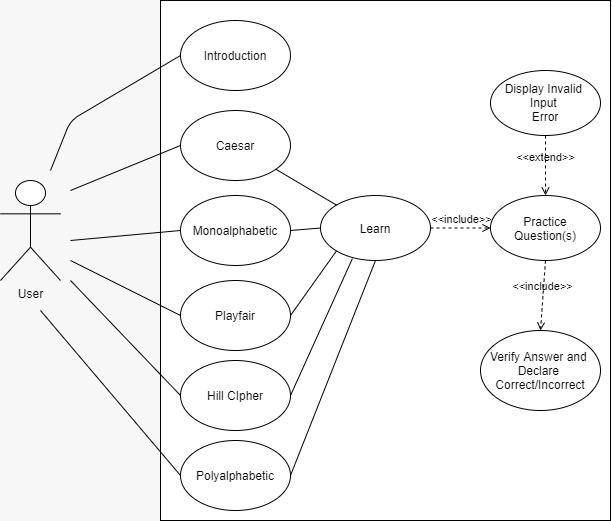
1. **Sequence Diagram**

****

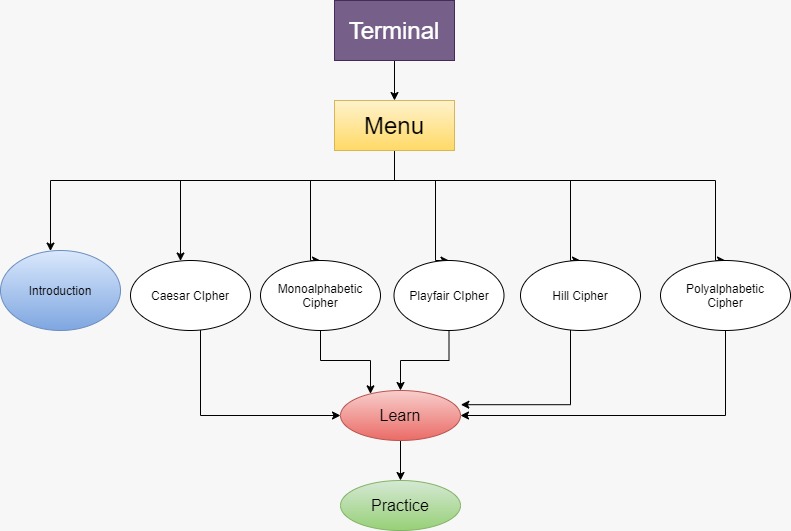
1. **State Chart Diagram**



1. **Use case Diagram**

****

1. **System Outline Diagram**

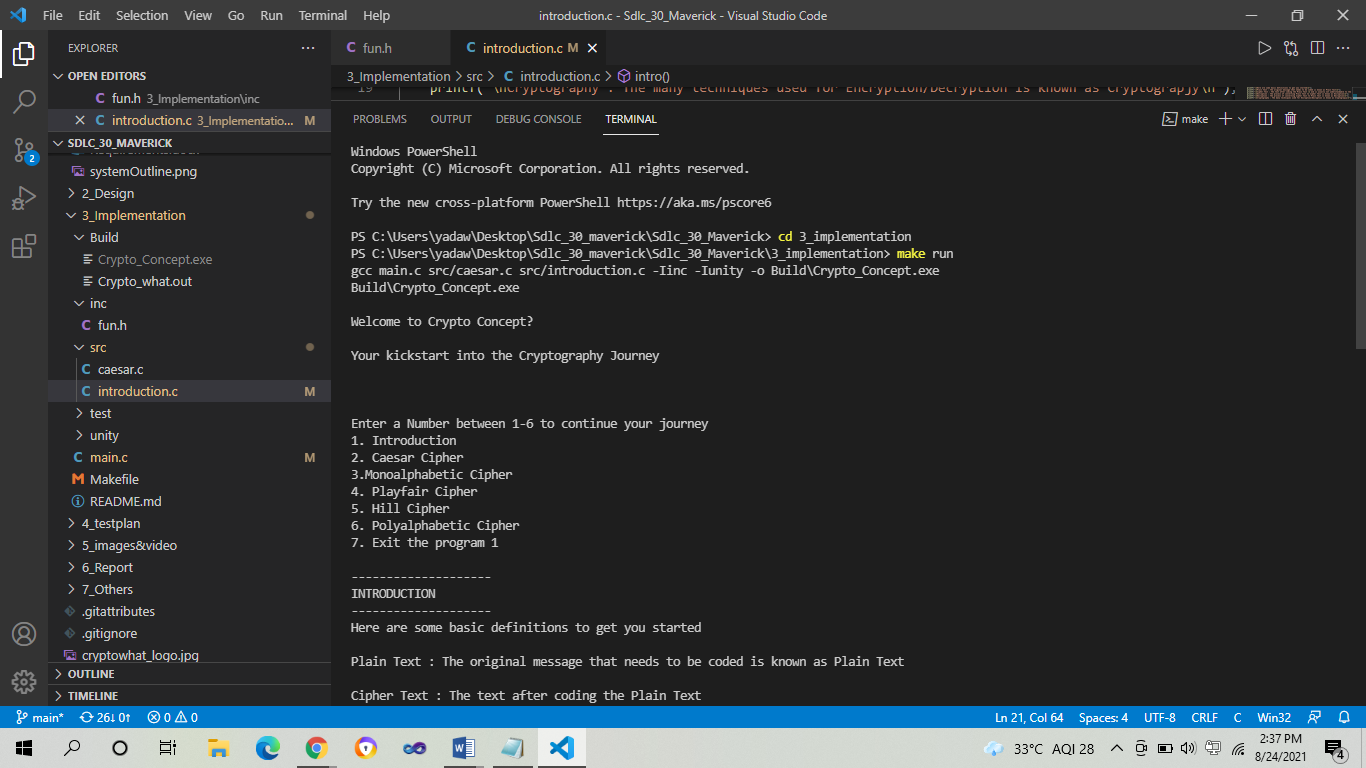


**Test Plan**

**Low level Requirement:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Test ID** | **Description** | **Exp. I/P** | **Exp. O/P** | **Actual O/P** | **Type of Test** |
| L\_01 | User enters the right answer for encryption | Only alphabets, no spaces, right answer | CORRECT\_ANSWER | CORRECT\_ANSWER | Requirement based |
| L\_02 | User enters the wrong answer for encryption | Only alphabets, no spaces, wrong answer | WRONG\_ANSWER | WRONG\_ANSWER | Requirement based |
| L\_03 | User enters digits/other characters too for encryption | No spaces | INVALID\_INPUT | INVALID\_INPUT | Requirement based |
| L\_04 | User enters the right answer for decryption | Only alphabets, no spaces, right answer | CORRECT\_ANSWER | CORRECT\_ANSWER | Requirement based |

**Output Images**

****

