**HEMVATI NANDAN BAHUGUNA GARHWAL UNIVERSITY**

(A Central University) Srinagar Garhwal, Uttarakhand

**School of Engineering and Technology**



Session (2021 - 2022)

A PROJECT REPORT ON

**“Encryption & Decryption of Message”**

Submitted in Partial fulfillment for the award of the degree of Bachelor of Technology

in Computer Science and Engineering HNBGU, Srinagar Garhwal (Uttarakhand)

**Guided By:- Submitted By:-**

Vijay Bijalwan Sir Name - **Rohit Kumar ( 19134501029)**

Assistance Professor B.Tech (C.S.E.) – 6th Sem.

Dept. of Computer Science and Engg.

#### DECLARATION :

I, **Rohit Kumar** bearing the **roll no** **19134501029** student of Computer Science and Engineering Department at Hemvati Nandan Bahuguna Garhwal University (A CentralUniversity), Srinagar (Garhwal), Uttarakhand, submit this project report entitled“**ENCRYPTION & DECRYPTION OF MESSAGE**” to Computer Science and EngineeringDepartment, Hemvati Nandan Bahuguna Garhwal University, for the award of the **Bachelors of Technology degree in ComputerScience & Engineering** and declaring that the work done is genuine and produced under the guidance of **Mr. Vijay Bijalwan**, Department of Computer Science and Engineering, Hemvati Nandan Bahuguna Garhwal University.

**DATE: 17/08/2022**

**PLACE: Srinagar ( Chauras)**

**Student Name**

Rohit Kumar ( 19134501029 )

#### CERTIFICATE

This is to certify that, this project report titled “**ENCRYPTION & DECRYPTION OF MESSAGE**” submitted by **“Rohit Kumar”** bearing roll no **19134501029** is bonafide record of the work carried out by him in partial fulfilment for the requirement of the award of **Bachelor of Technology** in **Computer Science and Engineering** degree from Hemvati Nandan Bahuguna Garhwal University (A Central University) at Srinagar (Garhwal), Uttarakhand.

**Mr. Vijay Bijalwan**

Department of Computer Science & Engineering Hemvati Nandan Bahuguna Garhwal University (A Central University)

Srinagar (Garhwal), Uttarakhand

#### ACKNOWLEDGEMENT

I would like to express my deepest gratitude to all people for sprinkling their help and kindness in the completion of this Project. I would like to start this moment by invoking my purest gratitude to **Mr. Vijay Bijalwan** , Department of Computer Science and Engineering, Hemwati Nandan Bahuguna Garhwal University (A Central University), Srinagar (Garhwal), Uttarakhand, my project instructor.

The completion of this project could not have been possible without his expertise and invaluable guidance in every phase at Hemvati Nandan Bahuguna Garhwal University (A Central University), Srinagar (Garhwal), Uttarakhand for helping me.

I would like to thank **Prof. M.M.S Rauthan, Prof. Y.P Raiwani**, all the lab assistants and other staffs of Computer Science and Engineering Department, Hemvati Nandan Bahuguna Garhwal University (A Central University), Srinagar (Garhwal), Uttarakhand, for their kind support. Last but not least, I would like to thank my parents and my friends for their unwavering belief despite ups and downs in my journey.

### ABSTRACT

The purpose of this study was to develop a “**encryption & decryption of message”** to to achive data message security and privacy by which ease the process of doing this job than earlier pen and paper-based management. So, the development of a software application –‘Encrption & Decryption’introduces the automation in the organizations serving this purpose.

This project is carried out as a partial fulfilment of the degree of B.Tech. Nowadays this kind of application is very essential for any small or medium sized organization. An Accountant, regardless of the number of Staff and Student, must maintain all records pertaining to payment/fees system digitally.

This application will help to encrypt and decrypt the text message / data or Information that help us to

Secure the data and information..

### CONTENTS

CANDIDATE’S DECLARATION… i

[CERTIFICATE ii](#_bookmark0)

[ACKNOWLEDGEMENT iii](#_bookmark1)

[ABSTRACT ………………………………………………………………………… iv](#_bookmark2)

1. About My Project ……………………………………………………………………… 01
2. [Introduction to my web Application 02](#_bookmark3)

Problem definition Solution

1. [Caesar Cipher 7](#_bookmark4)

Encryption

Decryption

1. *PlayfairCipher…………………………*

Encryption

Decryption

###### System design ……………………

###### 4..Code 12-45

1. *System testing 46- 47*

Unit testing Integration testing

User acceptance testing

###### Implementation 48-53

Sample screenshots

###### Conclusion 53-54

1. *References 55*

1. **ABOUT BY PROJECT**

*“The goal of creating this website is to secure message or information.”*

I used the cryptographic

I Created project for the Purpus of Encryption and decryption of Text messages or Data or Information

to providethe security of data .

This project is used by the key which may be public or private . We will use encryption and decryption

method to by using the several algorithms . it will having sender the the receiver , the sender

send the plain text message .

The interior process is that Used some key and plain text and some algorithms to encrypt

and decrypt the messages .

When Receiver used the key then cipher text(Encrypted message)

will decrypted and that will be same as the same message that Sender sended.

This is a web Application , created by me using **HTML**, **CSS**, ans **JavaScript** and also

I did try to create a better User Interfare from that user directly interect with this web Application .

I have used the CSS for the better Styling the WebPage and use the Propery of CSS like flex , grid , backgroung ,margin etc

I have several algorithm in JavaScript for the used in Matrix Operation of the Playfair Cipher.

In also add Event Handler in the web web page that create an effect by clicking on the page.

I have Used Playfair cipher and Caesar Cipher for the securing the Messages.

I have deployed this web application on the github . and the github link is below…

**Github web Link *:*** [*https://rohitkr01.github.io/Enquei/*](https://rohitkr01.github.io/Enquei/)

# 2. Introduction to My Application

### Problem definition

In this project, I am securing a message by a key , and receiver dencrypt that message to get the original palin text message that can understable by the user(human Language)..

Problem is that , how can we secure the message and what would be approach to acheive the this security goal.? To solve this problem Discuss the entire process , Expain it.

### Solution

To secure the text message or data or Information , I will use cryptograghy methos . Cryptography is used

to secure and protect data during communication. It is helpful to prevent unauthorized person or group

of users from accessing any confidential data.

Encryption and decryption are the two essential functionalities of cryptography.

Encryption is one the most effective approach to achieve **data security and privacy**. The Encryption

techniques hide the original content of a data in such a way that the original information is recovered

only through using a key known as decryption process.

#### I am having Two Methos for Encryption and Decryption od Message :

1. **Caesar cipher**
2. **Playfair Cipher**

Caesar Cipher :

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It’s simply

a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of

positions down the alphabet.

For example with a shift of 1, A would be replaced by B, B would become C, and so on.

##### HOME

Enter the plain Text

Select Shift Number

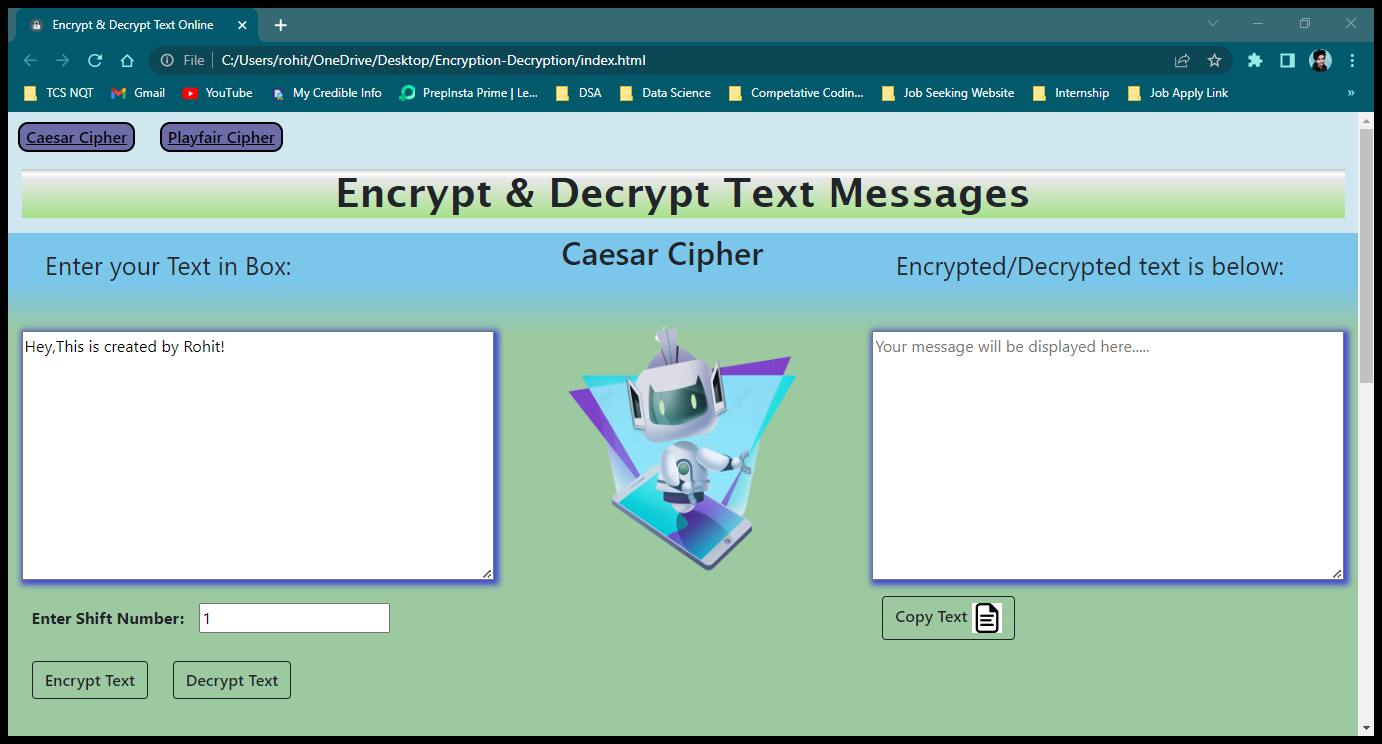
Tap on the encrypt button.

You Encrypted message will see on right side Box .

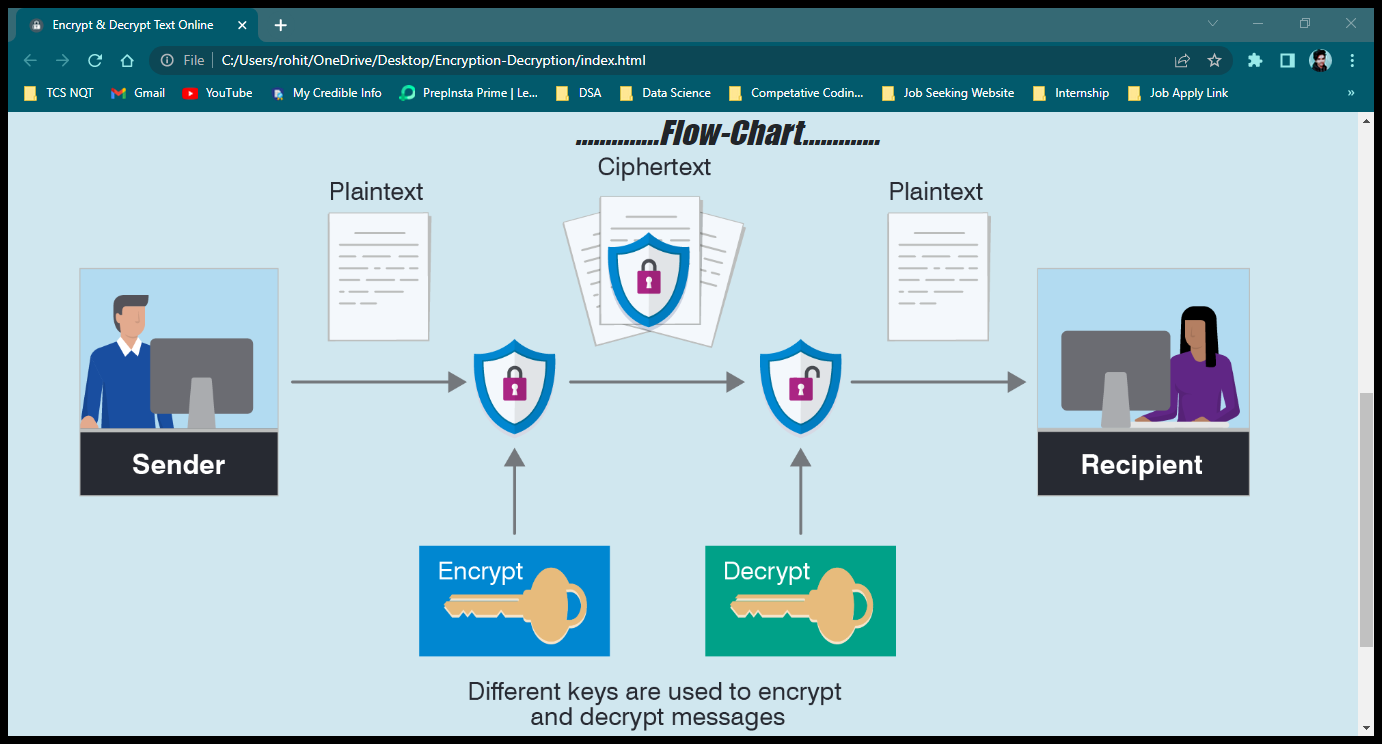
Copy the encrypted message and paste it in left side input Box the after

Tap on the decrypt button .

You will see the the decrypted massage that will be same as the original Message.

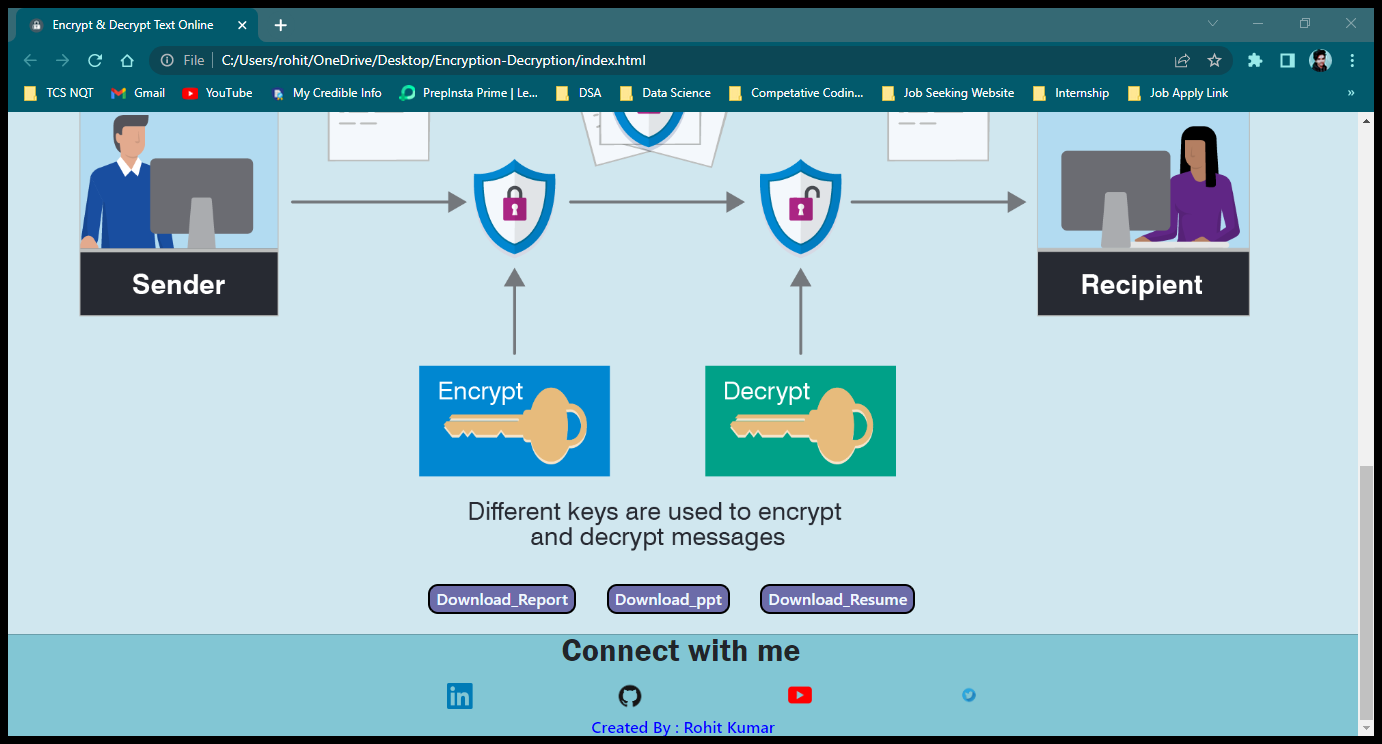


I have also Mentioned the flow Diagram in website that show how the Caesar cipher work .



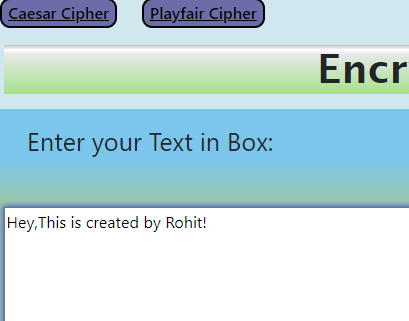
You can also download my PPT , Report File also my Resume by pressing on that particular Button .

Ans also you can Connect with me via social media , by pressing on the particular social media buttons.





When Tap on the Playfair Cipher Button , it will redirect you to playfair cipher page..



Then after the page of Playfair Cipher will appear .

**PlayFair Cipher :**

The Playfair cipher was the first practical **digraph**(*pair of alphabets*) substitution cipher.

The scheme was invented in 1854 by Charles Wheatstone but was named after Lord Playfair who promoted the use of the cipher.

In playfair cipher unlike traditional cipher we encrypt a ***pair of alphabets***(digraphs) instead of a single alphabet.

**Encryption Technique :**

The Playfair algorithm is based on the use of a 5\*5 matrix of letters constructed using a key.

We need :

Key

Plaintext

The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a LAST alphabet is added

to the last letter.

The Playfair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.

**The Algorithm consistes of 2 steps:**

1. Generate the key Square(5×5) at the receiver’s end:

o The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext.

Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is

omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J,

then it is replaced by I.

o The initial alphabets in the key square are the unique alphabets of the key in the order in

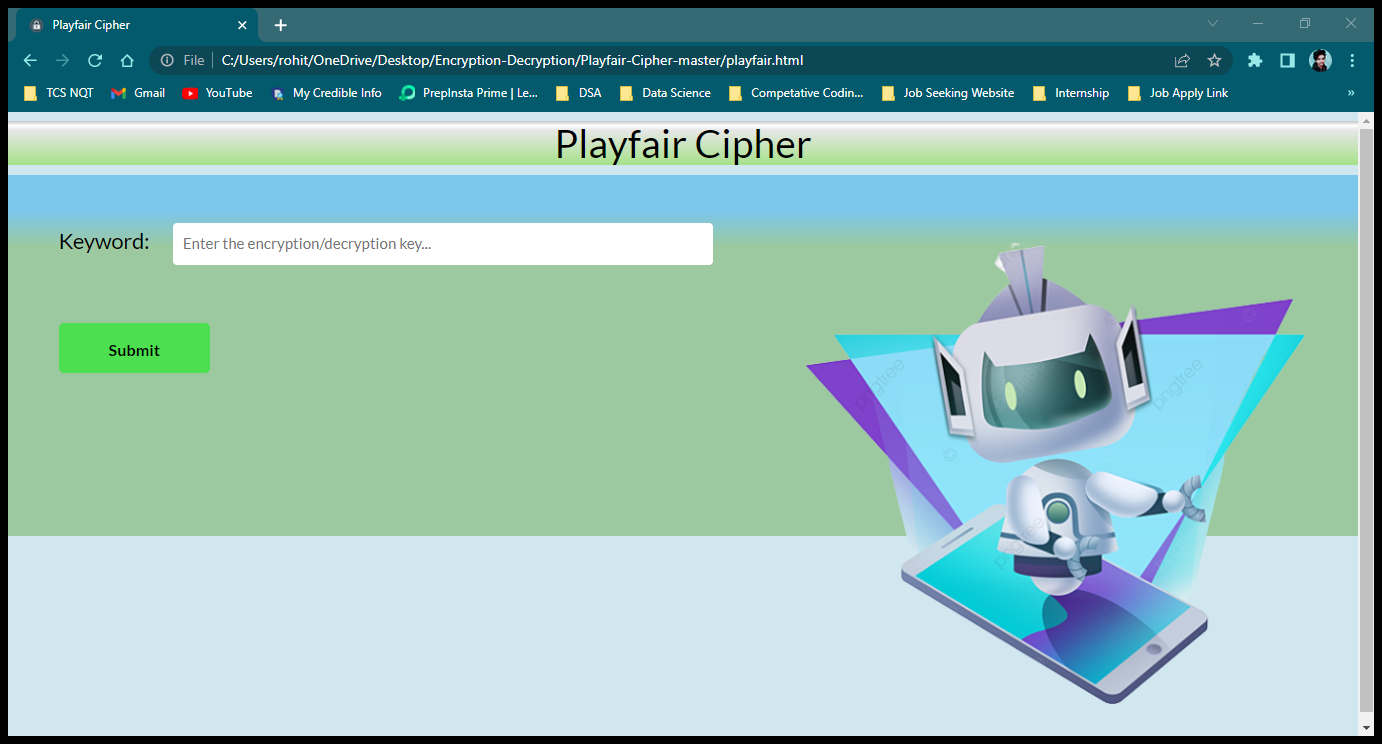
which they appear followed by the remaining letters of the alphabet in order.

Note: For both encryption and decryption, the same key is to be used.

1. Algorithm to decrypt the ciphertext:

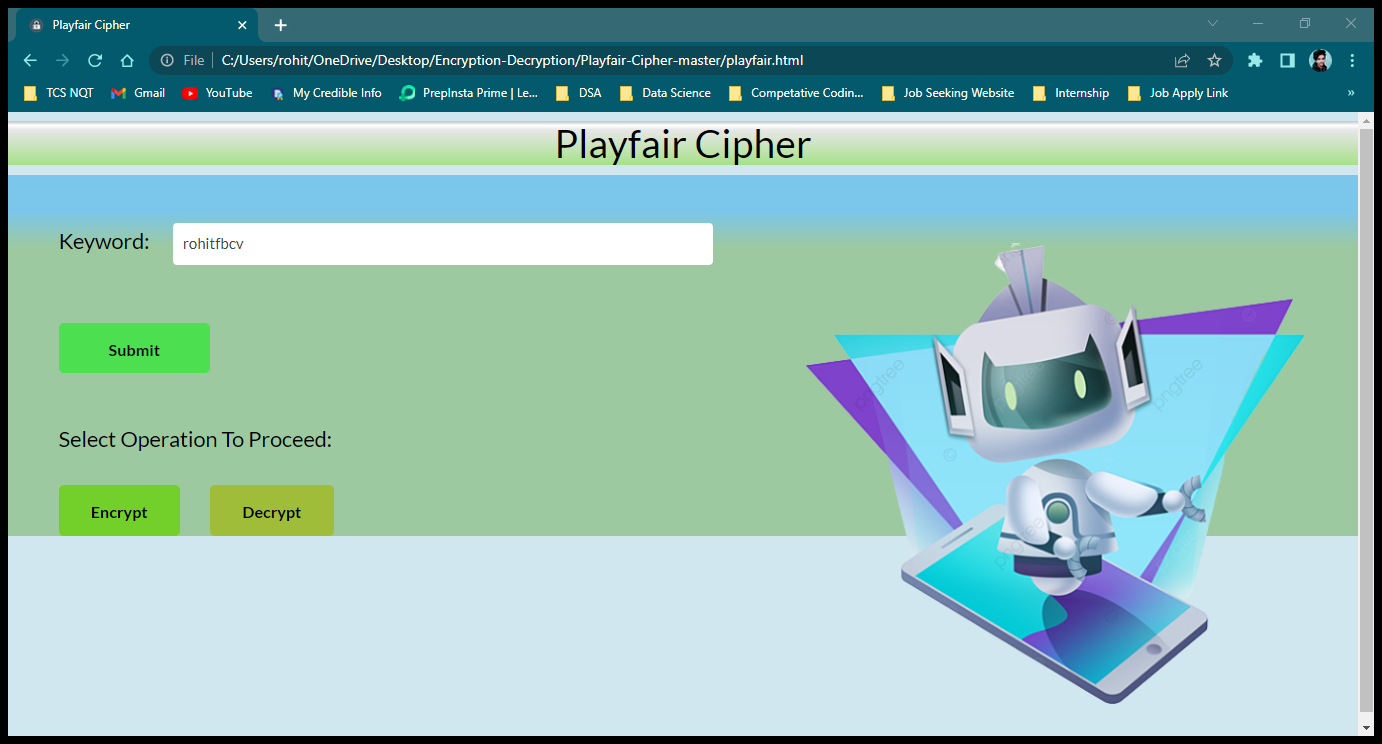
The ciphertext is split into pairs of two letters (digraphs).

Note: The ciphertext always have even number of characters.



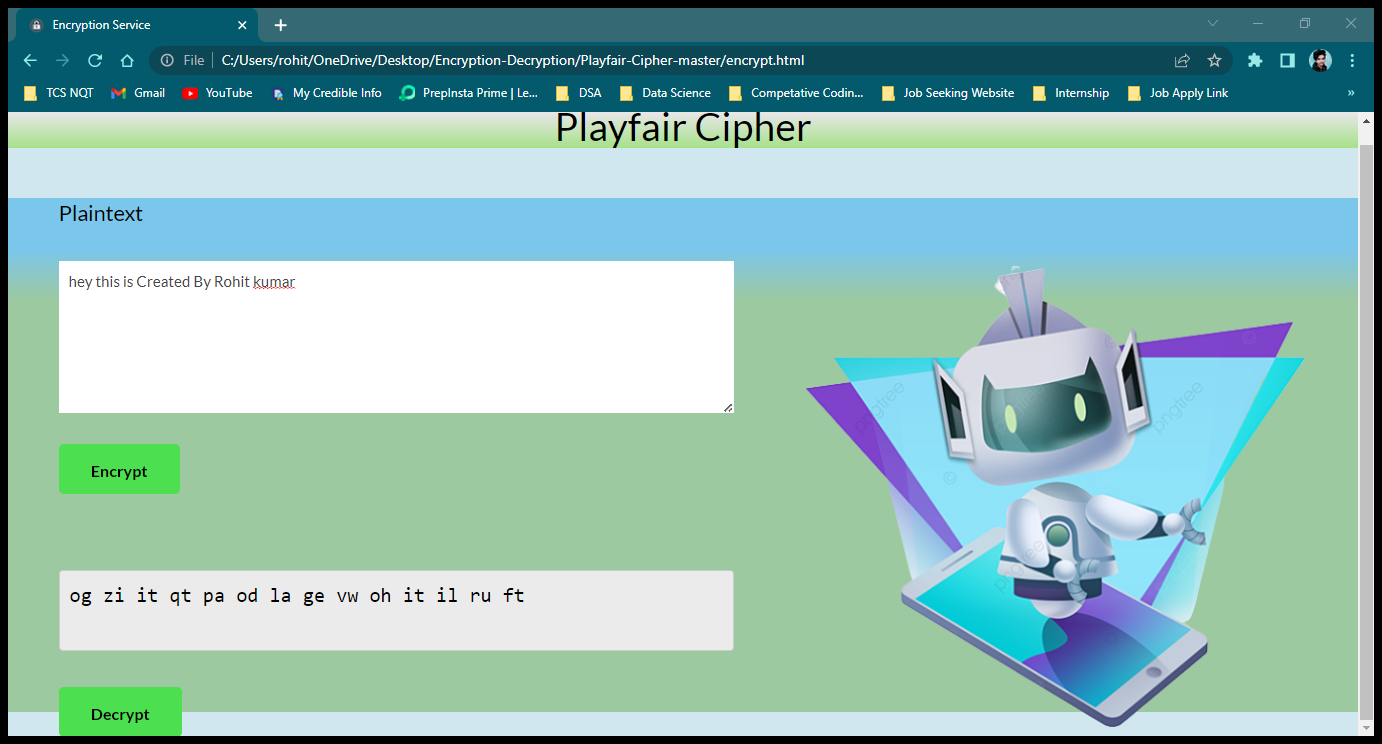
Enter the Key

Press the Submit button



Then after Pressing On the Encrypt Button

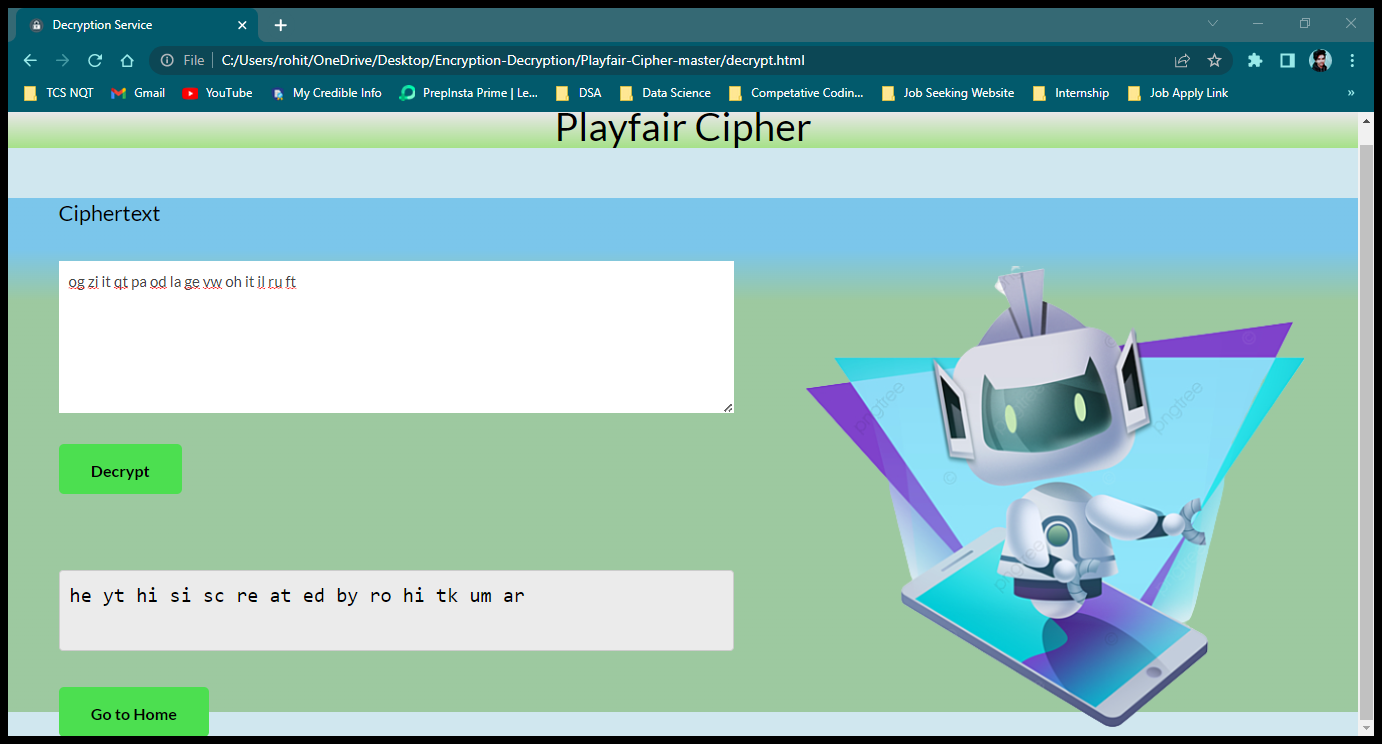
I will see encrypted message in below box .



Copy the encrypted message and paste it in the box

Press on the Decrypt Button

I will see the Decrypted Message that is same as the Original Message .



When I Press on the Go to home Button , it will redirect on the the home page of the

# SYSTEM ENVIRONMENT

#### Requirement analysis: -

Conceptually, requirements analysis includes three types of activities:

Eliciting requirements:(e.g., the project charter or definition), business process documentation, and stakeholder interviews. This is sometimes also called requirements gathering or requirements discovery.

Analysing requirements: determining whether the stated requirements are clear, complete, consistent and unambiguous, and resolving any apparent conflicts.

Recording requirements: Requirements may be documented in various forms, usually including a summary list and may include natural-language documents, use cases, user stories, process specifications and a variety of models including data models.

Requirement's analysis can be a long and tiring process during which many delicate psychological skills are involved. Large systems may confront analysts with hundreds or thousands of system requirements. New systems change the environment and relationships between people, so it is important to identify all the stakeholders, take into account all their needs and ensure they understandthe implications of the new systems. Analysts can employ several techniques to elicit the requirementsfrom the customer. These may include the development of scenarios (represented as user stories in agile methods), the identification of use cases, the use of workplace observationor ethnography, holding interviews, or focus groups (More aptly named in this context as requirements workshops, or requirements review sessions) and creating requirements lists. Prototyping may be used to develop an example system that can be demonstrated to stakeholders. Where necessary, the analyst

will employ a combination of these methods to establish the exact requirements of the stakeholders, sothat a system that meets the business needs is produced. Requirement's quality can be improved through these and other methods

Visualization. Using tools that promote better understanding of the desired end-product such as visualization and simulation.

Consistent use of templates. Producing a consistent set of models and templates to document the requirements.

Documenting dependencies. Documenting dependencies and interrelationships among requirements, as well as any assumptions and congregations.

The system should also embrace the following requirements:

* **User-friendly**: The system must accommodate a clearly understandable user interface as well as documentation help at any stage of the user interaction with the system.
* **Security:** The system should be designed to make it impossible for anybody to logon without a valid username and password. Data encryption should be employed to keep the user login name and password secret.
* **Reliability:** The system would be used by the accounting section of any organisation. Since this application is subject to process monetary matters, this must be reliable to the users of this application.
* **Ease of Use:** The views and operations should be easy to use and intuitive. Documentation should be provided.
* **Performance:** The system should have a quick response time.
* **System requirements:** This system would be designed to run on a minimum hardware configuration like 500MHz x86 machines. Considering the vast hardware available nowadays, this would not pose any problems.

**Hardware Requirements**

The hardware minimum and maximum recommended requirements are listed below:

|  |  |  |
| --- | --- | --- |
| **Hardware** | **Minimum Recommended**  **Requirements** | **Maximum Recommended**  **Requirements** |
| Internal Memory (RAM) | 2.00 GB | 3.00 GB or Higher |
| Hard Disk Capacity (CPU) | 60.00GB | 80.00GB or Higher |
| Processor | Intel Pentium 1.60GHZ  Or AMD / Ryzen etc | Intel(R) Core i3 2.40 GHZ or Higher or any processor |
| Monitor | 17” Colored 32bit | 18” Colored or Higher 64bit |
| Video Card | 128MB AGP | 256 MB AGP or Higher |

*Table 2.1: Hardware Requirements*

**Software Requirements**

The software minimum recommended requirements and maximum recommended requirements are listed below:

|  |  |  |
| --- | --- | --- |
| **Software** | **Minimum Recommended Requirements** | **Maximum Recommended Requirements** |
| System type | Microsoft Win7 or XP 32bit Operating System | Microsoft Win10 64bit Operating System  Or any higher |
| Storage | FAT File System | NTFS File System |
| Programming Language  Compiler | HTML, CSS ,JavaScript  Windows 7 | HTML , CSS ,JavaScript  Windows 8 or Higher |

*Table 2.2: Software Requirements*

### System Development Life Cycle

System development life cycle is a process of developing software on the basis of the requirement of the end user to develop efficient and good quality software. It is necessary to follow a particular procedure. The sequence of phases that must be followed to develop good quality software is known as SDLC (system development life cycle).

As with most undertakings, planning is an important factor in determining the success or failure of anysoftware project. Essentially, good project planning will eliminate many of the

mistakes that would otherwise be made, and reduce the overall time required to complete the project. As a rule of thumb, the more complex the problem is, and the more thorough the planning process must be. Most professional software developers plan a software project using a series of steps generally referred to as the software development life cycle*.* A number of models exist that differ in the number of stages defined, and in the specific activities that take place within each stage. The following exampleis a generic model that should give you some idea of the steps involved in a typical software project.

*PHASES OF SDLC*

* System Analysis
* System Design
* Coding
* System Testing
* System Implementation
* System Maintenance

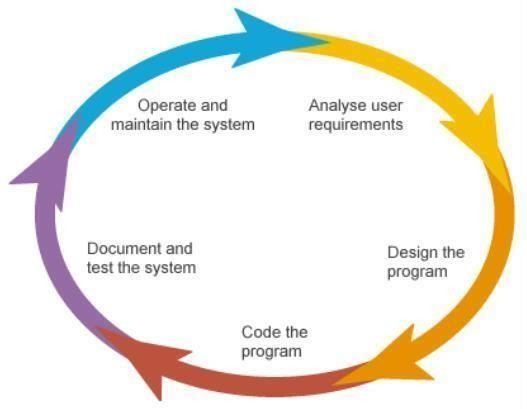


Fig. 1 : Phase of SDLC

Figure 2: Flowchart of SDLC

# SYSTEM ANALYSIS

**System Design:** The design document that we will develop during this phase is the blueprint of the software. It describes how the solution to the customer problem is to be built. Since solution to complex problems isn’t usually found in the first try, iterations are most likely required. This is true for software design as well. For this reason, any design strategy, design method, or design language must be flexible and must easily accommodate changes due to iterations in the design . Any technique or design needs to support and guide the partitioning process in such a way that the resulting sub-problems are as independent as possible from each other and can be combined easily for the solution to the overall problem. Sub-problem independence and easy combination of their solutions reduces the complexity of the problem.

Basic design principles that enable the software engineer to navigate the design process suggest a set of principles for software design, which have been adapted and extended in the following list:

Free from the suffer from "tunnel vision." A good designer should consider alternative approaches, judging each based on the requirements of the problem, the resources available to do the job.

The design should be traceable to the analysis model. Because a single element of the design model often traces to multiple requirements, it is necessary to have a means for tracking how requirements have been satisfied by the design model.

The design should not repeat the same thing. Systems are constructed using a set of design patterns, many of which have likely been encountered before. These patterns should always be chosen as an alternative to reinvention. Time is short and resources are limited! Design time should be invested in representing truly new ideas and integrating those patterns that already exist.

The design should "minimize the intellectual distance" between the software and the problem as it exists in the real world. That is, the structure of the software design should (whenever possible) mimicthe structure of the problem domain.

The design should exhibit uniformity and integration. A design is uniform if it appears that one person developed the entire thing. Rules of style and format should be defined for a design team before designwork begins. A design is integrated if care is taken in defining interfaces between design components.

The design activity begins when the requirements document for the software to be developed is available. This may be the SRS for the complete system, as is the case if the waterfall model is being followed or the requirements for the next "iteration" if the iterative enhancement is being followed or the requirements for the prototype if the prototyping is being followed. While the requirements specification activity is entirely in the problem domain, design is the first step in moving from the problem domain toward the solution domain. Design is essentially the bridge between requirements specification and the final solution for satisfying the requirements.

The design of a system is essentially a blueprint or a plan for a solution for the system. We consider a system to be a set of components with clearly defined behaviour that interacts with each other in a fixed defined manner to produce some behaviour or services for its environment. A component of a system can be considered a system, with its own components. In a software system, a component is a software module.

The design process for software systems, often, has two levels. At the first level, the focus is on deciding which modules are needed for the system, the specifications of these modules, and how the modules should be interconnected. This is what is called the system design or top-level design. In the second level, the internal design of the modules, or how the specifications of the module can be satisfied, is decided. This design level is often called detailed design or logic design. Detailed design essentially expands the system design to contain a more detailed description of the processing logic and data structures so that the design is sufficiently complete for coding.

Because the detailed design is an extension of system design, the system design controls the major structural characteristics of the system. The system design has a major impact on the testability and modifiability of a system, and it impacts its efficiency. Much of the design effort for designing software is spent creating the system design.

The input to the design phase is the specifications for the system to be designed. Hence, a reasonable entry criterion can be that the specifications are stable and have been approved, hoping that the approval mechanism will ensure that the specifications are complete, consistent, unambiguous, etc. The output of the top-level design phase is the architectural design or the system design for the software system to be built. This can be produced with or without using a design methodology. A reasonable exit criterion for the phase could be that the design has been verified against the input specifications and has been evaluated and approved for quality.

CODE

ystem testing is the stage of implementation, which is aimed at ensuring that the system works accurately and efficiently before live operation commences. Testing is the process ofexecuting the program with the intent of finding errors and missing operations and also a complete verification to determine whether the objectives are met and the user requirementsare satisfied. The ultimate aim is quality assurance. Tests are carried out and the results are compared with the expected document. In the case of erroneous results, debugging is done. Using detailed testing strategies, a test plan is carried out on each module. The various testsperformed are unit testing, integration testing and user acceptance testing.

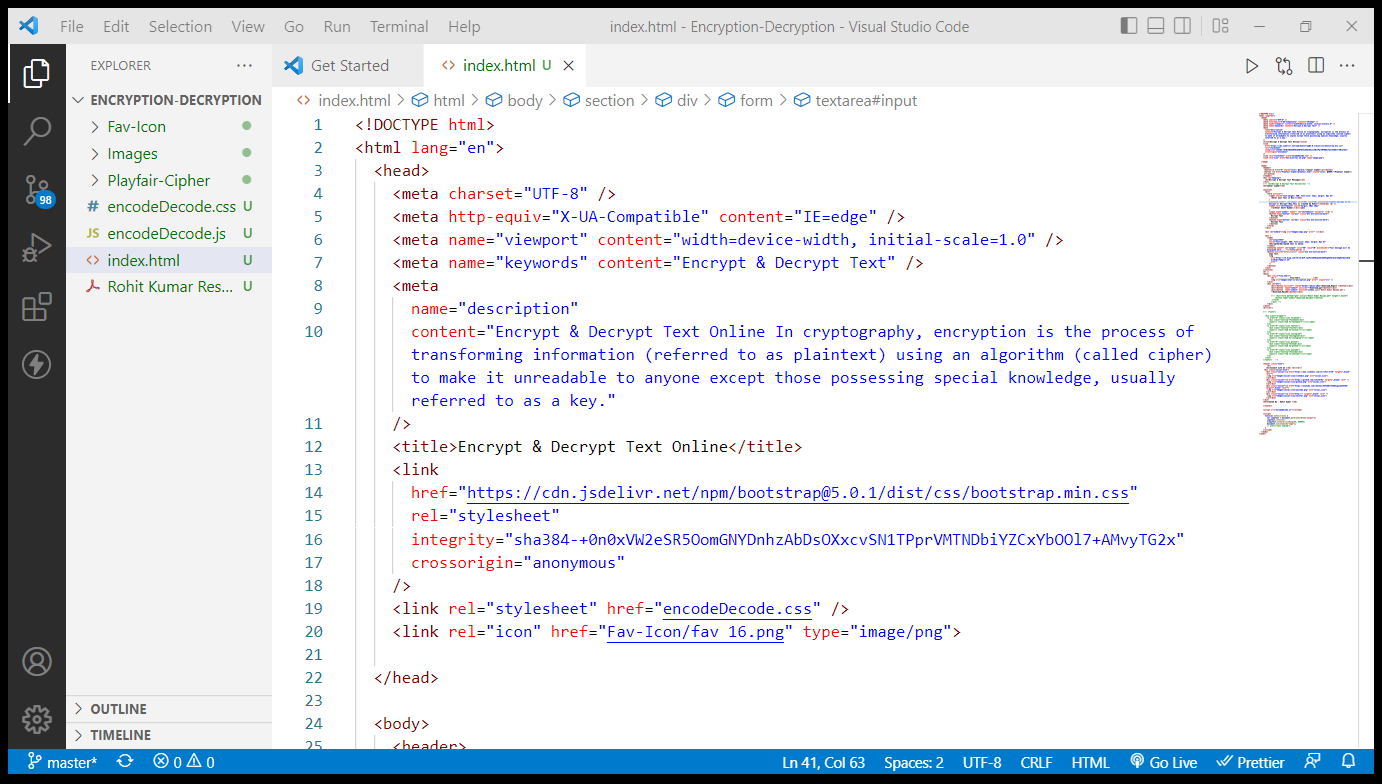
### Unit Testing

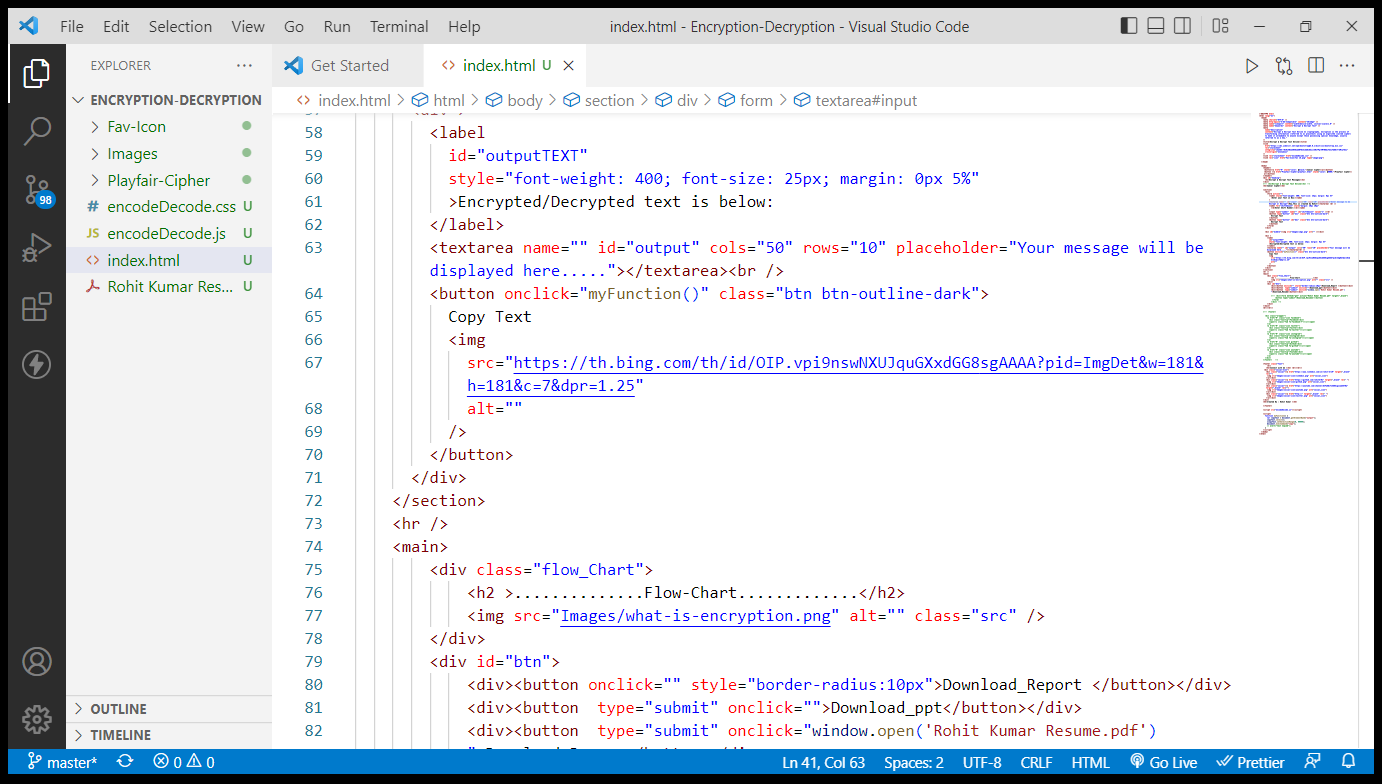
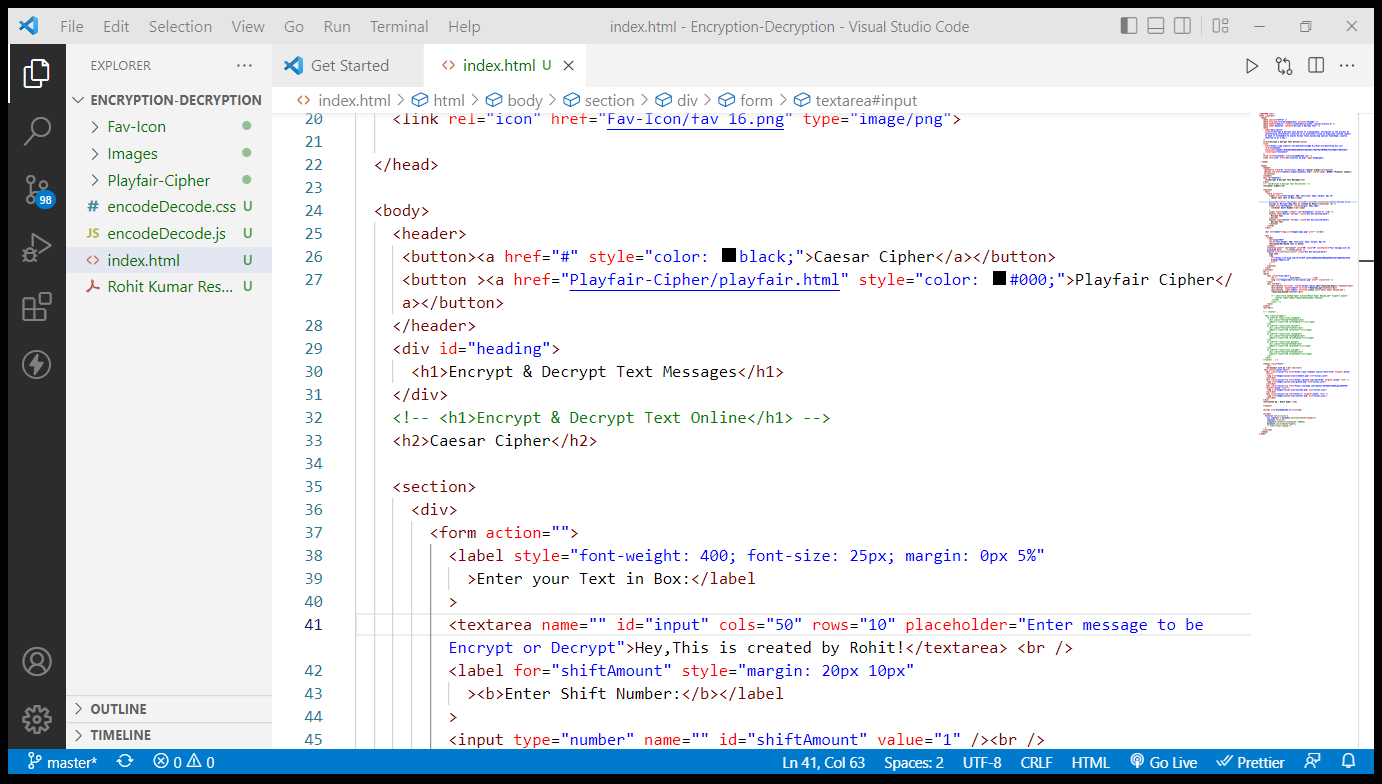
The software units in a system are modules and routines that are assembled and integrated to perform a specific function. Unit testing focuses first on modules, independently of one another, to locate errors. This enables, to detect errors in coding and logic that are contained within each module. This testing includes entering data and ascertaining. The various controlsare tested to ensure that each performs its action as required.

### Integration Testing

Data can be lost across any interface, one module can have an adverse effect on another, sub functions when combined, may not produce the desired major functions. Integration testing is a systematic testing to discover errors associated within the interface. The objective is to take unit tested modules and build a program structure. All the modules are combined and tested asa whole. This testing provides the assurance that the application is well integrated functional unit with smooth transition of data.

**Code Screen Shot**

****

****

User acceptance of a system is the key factor for the success of any system. The system under consideration is tested for user acceptance by constantly keeping in touch with the system users at time of developing and making changes whenever required.

### Test Results

All the test cases mentioned above passed successfully .No defects encountered .

# IMPLEMENTATION

Implementation is the stage in the project where the theoretical design is turned into a workingsystem and is giving confidence on the new system for the users that it will work efficiently andeffectively. It involves careful planning, investigation of the current system and its constraints on implementation, design of methods to achieve the changeover, an evaluation of change over methods. Apart from planning major task of preparing the implementation are education and training of users. The implementation process begins with preparing a plan for the implementation of the system. According to this plan, the activities are to be carried out, discussions made regarding the equipment and resources and the additional equipment has to be acquired to implement the new system.

Implementation is the final and the most important phase. The most critical stage in achieving a successful new system is giving the users confidence that the new system will work and be effective. The system can be implemented only after thorough testing is done and if it is found to be working according to the specification.

### 

### 7 CONCLUSION

The objective of this research was to design and development a user friendly ‘Encryption & Decryption’.

My Web Application contain the Best User Interface where user interact more .

* This application is useful not for only ‘MAU’, but also any other organization who are keen to utilize this kind of software.
* It can be operated very easily. There is no need to recruit extra dedicated person or equipment to handle this application.
* It provides very high level user friendly function. Though we already added maximum features to this application, we are willing to make the application more flexible and professional.

1. ***LIMITATIONS***

The limitations of the application are as follows:

* + In this project there is no specified credential for User Sender , Receiver and for Administration in my application.
  + We worked with onlytesting arbitrary data, so the application is not tested with large scale real data which help to find bugs easily.
  + Reports are not generated in other application such as Excel, PDF etc.
  + No such more encryption algorithms is used .
  + Different database connection procedure is complex. Here I used only Files.
  + In this application the coding structure is simple

1. *FUTURE SCOPE*

In future we will overcome current limitations implement the following issues:

1. We can develop the web application in JavaScript or MYSQL.
2. Applying the SSL (Secure Socket Level) for production server.
3. Implementing user management system according permission level.
4. Appling time and skill reducing techniques.
5. Generating report in other application like Excel, PDF etc.
6. Merging modules.

54

9. REFERENCES

[1]. [www.academia.edu/](http://www.academia.edu/)

[2]. [Caesar Cipher in Cryptography - GeeksforGeeks](https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/)

[3]. https://en.wikipedia.org/wiki/Playfair\_cipher