CipherByte

A PROJECT REPORT

Submitted By

Sayak Chatterjee (20BCS1452)

in partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE ENGINEERING

Chandigarh University

June-July 2022

CHANDIGARH UNIVERSITY
Discover. Learn. Empower.

BONAFIDE CERTIFICATE

Certified that this project report **CipherByte** is the bonafide work of Sayak Chatterjee with UID 20BCS1452 who carried out the project.

HEAD OF DEPARTMENT **SUPERVISOR**

SIGNATURE **SIGNATURE**

Department
Computer Science Engineering

Submitted for the project viva-voce examination held on —-----------------------------

INTERNAL EXAMINER **EXTERNAL EXAMINER**

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Cyber security is a discipline that covers how to defend devices and services from electronic attacks by nefarious actors such as hackers, spammers, and cybercriminals. While some components of cyber security are designed to strike first, most of today's professionals focus more on determining the best way to defend all assets, from computers and smartphones to networks and databases, from attacks.Cyber security has been used as a catch-all term in the media to describe the process of protection against every form of cybercrime, from identity theft to international digital weapons. These labels are valid, but they fail to capture the true nature of cyber security for those without a computer science degree or experience in the digital industry. Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems. Without a cybersecurity program, your organization cannot defend itself against data breach campaigns, which makes it an irresistible target for cybercriminals.he fact of the matter is whether you are an individual, small business, or large multinational, you rely on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones, and the Internet of Things (IoT) and we have a myriad of potential security vulnerabilities that didn't exist a few decades ago. We need to understand the difference between cybersecurity and information security, even though the skillsets are becoming more similar.

ABBREVIATIONS

Abbreviation	Full Name
HTML	Hyper Text Markup Language
CSS	Cascading Style Sheets
DB	Data Base
SQL	Structured Query Language
API	Application Programming Interface

CHAPTER 1: INTRODUCTION

Cybersecurity's importance is on the rise. Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow. Data leaks that could result in identity theft are now publicly posted on social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive. The fact of the matter is whether you are an individual, small business, or large multinational, you rely on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones, and the Internet of Things (IoT) and we have a myriad of potential security vulnerabilities that didn't exist a few decades ago. We need to understand the difference between cybersecurity and information security, even though the skillsets are becoming more similar. With time cybercrime is increasing and Cybercriminals are becoming more sophisticated, changing what they target, how they affect organizations, and their methods of attack on different security systems.

1.1 NEED IDENTIFICATION / IDENTIFICATION OF RELEVANT CONTEMPORARY ISSUE

With the vision of a trillion-dollar digital component, accounting for one-fifth of the $5-trillion national economy, the importance of cyberspace in India would only keep growing as Indians are consuming the internet at a faster pace than ever compared to the earlier trends of the same, driven by affordable tariffs, low-cost smartphones and a spurt in availability of audio-visual content in Indian languages. Financial services, payments, health services, etc are all connected to digital mediums; and due to Covid-19, this is expected to increase. There has been a rapid increase in the use of the online environment where millions of users have access to internet resources and are providing content on a daily basis. To ensure critical infrastructure systems do not collapse under any situation.To ensure Business continuity. For the success of government initiatives like Digital India, Make in India and Smart Cities. To balance Individual’s rights, liberty and privacy cybersecurity is needed, and a a project towards encryption algorithms helps in better understanding of the issues and making the whole process on the internet communication more strong and secure.

1.2 IDENTIFICATION OF PROBLEM

There are many problems due to which encryption algorithms are being used these days at a faster pace in the online development process, be it storing data into the database or to make the communication between two parties more secure.

I. SESSION HIJACKING:

Session hijacking stands for a cyberattack where a malicious hacker places himself in between your computer and the website’s server while you are engaged in an active computer session (the time between you first log into your bank account, and then log off after your operation, for example) in order to steal it. The hacker actively monitors everything that happens on your account, and can even kick you out and take control of it. This attack can be used to steal user data and the messages that are being transferred hence compromising the privacy of the user

II. SQL INJECTION ATTACKS:

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior. In this case if the database is exploited by the attacker and the important information in the database is stored in plain text this would lead to easy compromise of data.

III. INTERNET FOOTPRINTING:

This technique is used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best methods of finding vulnerabilities. The process of cybersecurity footprinting involves profiling organizations and collecting data about the network, host, employees and third-party partners. In this case a lot of information can be extracted by the attacker and if the data present on the system in plain text it would lead to all the data being revealed without any checks.

1.3 ORGANIZATION OF REPORT

The following is the structure that gives a brief overview about the report to the reader and the different sections containing different components of the development process.

I. Chapter 1: Introduction

The first chapter of the report helps in basic understanding of the whole project, the reasons behind development of such a concept along with giving a brief insight to the reader about the aims that the project wants to achieve along with the features the platform offers to the users to make the user experience better along with providing features that help in solving the problems that the project was developed to solve. Along with highlighting the key problems that the platform tries to solve defines the target audience for the project.Once the reader is sure about the type of audience being targeted they can have a clear idea of how the project is useful for the same in solving some major problems.

II. Chapter 2: Literature review

This section of the report helps in putting forward the readings and the training that were referred to in order to develop the concept behind the platform along with giving an opportunity to improve upon the idea as well as the concept therefore developing something better that has been developed in the past, leveling it up, increasing the efficiency along with covering a larger audience as the project can be developed in such a way in order to include the functionalities which is able to solve problems of not only those which such types of projects catered in the past hence making the project more useful.

III. Chapter 3: Design flow and process

This section talks about the period of training and how the experience and information gathered through the industrial training helped in overall concept generation that was needed in order to better understand cybersecurity and also understand the differences that having a well and secured system mean over the normal and vulnerable ones present out there.

IV. Chapter 4: Result analysis and validation

This section gives the final result of the training that is implementing the learning of the training into a project, the objectives that were converted to functionalities , diagrams representing the flow of control, and that of data among different sections of the project. It includes if the project works the way it was supposed to meet the requirements that were initially set during the initial phases. This part of the report tells about the tests that were done in order to verify the functionalities of the project and have a closer look on the fact if the learning of the industrial training is sufficient, validation of the data concept of the project and the code and the technologies being used.

V. Chapter 5: Conclusion and future scope

This section of the report helps in concluding the whole report, revisiting the points or the aim that the project was trying to achieve along with insights about if the platform was actually able to achieve those objectives successfully. It also gives the reader brief insight about the future scope of the project, basically telling the reader what the project aims to achieve in the future along with the changes that would be required in order to keep up with the changing needs of the users. This section also lists the links and names of all the references that were used throughout the report.

CHAPTER 2: LITERATURE REVIEW / BACKGROUND STUDY

Cybercrime is a serious threat that is on the rise. As we share more and more business and personal information online, criminals find new ways to steal and use that data for illegal purposes and financial gain. As this risk continues to grow in our daily lives, it's important to understand how cybercrime has become such a major problem, why we're all so vulnerable to it, and what steps we can take to protect ourselves. Cybercrime includes criminal activity that involves computers, networks, and digital devices. It can threaten and harm national security, businesses, and individuals. It is a wide scale problem that has affected many people's lives. Hence finding a solution to it has become a major concern in the present scenario and for the future to come as more and more modifications the technologies are going to go through and the advanced they get it is going to be even more difficult to prevent these technologies against cyberthreats as complexities make it even more hard to defend the systems in real time.

2.1 TIMELINE OF THE REPORTED PROBLEMS

Prior to 2010, cybersecurity was an insular domain. No one really cared, until something they were using didn't work. Devices blew up due to malware or adware, and users got annoyed when a machine disappeared to get reloaded by IT, but after the event was over, concern faded. As we entered the 2010s, most corporations acted the same way, but by 2018 and 2019, cybersecurity experts and security and risk pros became a fixture in boardrooms and newsrooms. The battle over "cyber" raged, and the resistance lost, so that's what it's called throughout. Consider this our surrender as we accept defeat with grace. Let's look at the last 10 years of notable security trends and events. Phrase Of The Decade: "We Take Your Privacy And Security Seriously". Everyone's heard or read this phrase, right before a company starts explaining how something happened that violates that privacy and security. And most security and risk pros recognize that the sentence above is missing a key word: "now" — "we take privacy and security seriously now."Excuse Of The Decade: "Sophisticated Attackers Bypassed Security Controls Etc." After the dust settled, what we almost always discovered is that the attackers weren't that sophisticated. Or if they were, they didn't have to flex too many mental muscles to get inside the environment. The combination of low-hanging fruit and living off the land provided all that attackers needed to breach the company.

2.2 PROPOSED SOLUTIONS

The evolution of cybersecurity has happened quickly and learning about the past can help inform us of the future. A long time ago in technology's past, the first-ever cyberthreats began to rear their heads as the computer began to make their mark. Known as "Creeper," this program could move across a network and leave traces of it everywhere it went. To counter, Ray Tomlinson created our first glimpse at cybersecurity by designing a program to hunt and delete Creeper, known as Reaper. As computers became more commercial and more everyday people began to use them, the need for security became more apparent as more viruses and threats surfaced. The next major innovation in cybersecurity came from the first major antivirus software in the US from John McAfee around in 1987. These innovations in security came at the perfect time, too, as the '90s would become known as the "Virus Era" because of the millions of computers that were infected in the decade due to the rise of internet usage. During this time, firewalls and antivirus software were the main sources of security that scanned incoming packets for malware and used immunizers—a tool that modified programs to trick viruses into thinking they were already infected—to stop infections from taking place. In the 2000s, cybercrime became more prominent as more of the world became more digital. World governments began to recognize and plan to stop cyberattacks and information security became a focus for businesses, people, and governments alike. Modern businesses are facing new kinds of threats that are evolving to beat new security systems and technology. To stay protected, businesses must have the latest tech, strategies, and tools.

2.3 BIBLIOMETRIC ANALYSIS

In 2014, Awoleye, Ojuloge and Ilori [8] carried out an analysis of e-government platforms to assess the possible flaws in the web servers. The average result was that 67% were affected by broken links, 43.8% with unencrypted passwords, 35% suffering from XSS and one out of four affected by SQL injection and cookie manipulation. In today's connected world, organizations rely heavily on their communications' infrastructure. For this reason, deployment of prevention technologies is very critical, but these technologies come with threats too. In 2014, Almadhoob and Valverde [9] designed a survey to understand how to assist small and medium organizations in Bahrain. These technologies should be supported by multiple layers including technical, management, and operation. The latest related work was in November 2014. The authors Zhao J. and Zhao S. [10] assessed the Fortune 500 organizations' e-commerce security. They performed analysis, audit and mapping for data collection and analysis. They found that most of the organizations posted security policies but only one third cannot clarify the security measures in action. In addition, all organizations used SSL to encrypt the traffic between the sites and users but only 16% limited the number of attempts to access to three tries. At last, all sites had firewalls to secure their perimeter. Nevertheless, there were few results of discovering computers operating systems of these organizations. In 2008, Alghathber, Mahmud and Hanif Ullah [4] used two open source vulnerability assessment tools Nikto and Nessus to evaluate about 169 Saudi Arabia's websites. They found that many of the websites were vulnerable to different types of attacks such as remote code execution, buffer overflow, denial of service and more. They recommended that organizations need a high level of security awareness and training about the use of secure coding. Also, they need to do vulnerability assessment frequently to discover new weaknesses in their systems and applications.

2.4 GOALS / OBJECTIVES

The goal of the training as well as the projects is to:

- Give a brief introduction about cybersecurity to the user
- Help the user to send messages including important information by converting them into ciphers
- To help the users have a secure method of communication.
- Develop a solution which is not only itself a stand alone project but also it is a concept that can be used embedded in other projects for better security and privacy.
- To give the project an algorithm which is easier to implement and provides a level of security that can be relied upon.

CHAPTER 3: DESIGN FLOW AND PROCESS

The training dealt with a lot of topics and covered them in a sequential manner over the course of 8 weeks. The whole training was distributed over 8 modules along with a mix of theoretical along with practical application. Theoretical lectures followed with practical applications of the same. There was in depth introduction to all the basic and key blocks of the ethical hacking , the basic requirements for the same along with concepts which could help in the case where advances technologies There were a huge amount of topics which were covered in such a way so that initial requirements of learning a skill was introduced and practiced beforehand, helping to understand the advanced concepts in a better manner.

3.1 CONCEPT GENERATION / EVALUATION OF DIFFERENT CONCEPTS AND FEATURES:

The training done was considered as a reference for concept generation of the project and following are the key components that were learned during the learning phase which can further be used in future.

1. Module: [Basics of security and computer networking]:

This module gives a basic introduction to hacking that what it actually is along with the types of hacking which are ethical and unethical. Along with giving a brief explanation about the types of hackers there exist. It also gives an insight about the methods or actions taken by different types of hackers in order to hack into a web application along with the key components needed for the same.

2. Module: [Information gathering and web development]

This module tells about the importance of the process of collecting data beforehand, so that before attacking or testing a particular website, the relevant information can be gathered which will help the attacking process as knowing the target better helps in understanding the ways the security can be modeled. It also gives a brief introduction about languages such as HTML, JavaScript and PHP which can be used in such a way in order to find the loopholes in the web application at the time of testing. It gives an idea about how web applications are made and how to create one, after knowing the process it becomes easier to locate loopholes.

3. Module: [Introduction to Web VAPT, OWASP and SQL]

VA stands for Vulnerability Assessment and PT stands for Penetration Testing. These two terms basically revolve around first that is tester tries to find all the vulnerabilities in the system and the second part tester tries to exploit all the vulnerabilities in the VA phase and record that how much damage a certain vulnerability can cause to the application and which vulnerabilities need to be fixed first can be decided based on the impact the vulnerability has on the website. This module also introduces us to a very important tool useful for ethical hackers that is OWASP (Open Web Application Security Project) which has all the information regarding the type of attacks that can take place on web applications along with the type of measures that can be taken to avoid those types of attacks.

4. Module: [Advanced web application attacks]

This module takes the attacks and how to perform them to an advanced level giving in depth information about how each attack works and how it can be used by an attacker for his or her own benefit. This module first gives an introduction about how a certain functionality works and how it can be used to make an attack take place once of the functionalities out of these which the module specifically focus on is filter bypassing as there are many types of filters on client side and server side.It tells us about the different encoding standards that are followed while development of web applications. It tells us about the vulnerability IDOR (Indirect Object Reference) and its cause, which is the rate limiting flaw .

5. Module : [Advanced web application attacks]

This module firstly gives an in depth introduction to session and cookies that are used for making secure connections between the user and the server. Further it tells about how these session and cookies can be used in order to exploit the connection between the user and the server, once this connection is exploited without the knowledge of the user it can be used in many ways such as tracking the movement of the person on the internet, fetching their personal information compromising their privacy while they are completely unaware of it

6. Module : [Identifying security misconfigurations and exploiting outdated web applications]

Firstly this module gives an introduction about what security misconfigurations actually are and how they can be exploited. Tells us about how the default settings in web applications from the developers side can lead to compromising crucial information about the web application. These default settings can be like the default error messages which are descriptive in nature and other settings such as the developer not changing default password for the authentication pages, making it easy for the hacker to guess those passwords.

7. Module : [Automating VAPT and secure code development]

This module tells us more about the importance of gathering relevant information beforehand regarding the organization we want to attack. The tools introduced by them were NMap, Dirbuster, Nikto and some others as well. It not only introduces these tools but also gives an in-depth knowledge of how to use these tools such as the NMap and Dirbuster and introduces various features and how they can be used to extract the information we need. These tools make the features automated which makes the whole testing process automated hence making it efficient.

8. Module : [Documentation and Reporting Vulnerabilities]

This module tells us about the importance of documentation in the testing phase. It's not only important to find all the vulnerabilities of the web application under test but also the fact that all these vulnerabilities need to be documented along with the proof that they exist and how much damage they can cause to the web application by showing the information that is being revealed by exploiting the vulnerability.

3.2 CONSTRAINTS

There were few constraints that were needed to be kept in mind while designing the platform and including the features into the platform. Different types of constraints played a major role in selecting features of the platform some of them are as follows:

- Firstly we needed to make sure that the information being provided on the website is correct.
- There were economic constraints as there were no external investors into the project and hence trying to use any paid features for the same was out of the scope of the project and hence such technologies needed to be used which were free and were trustable as well, this is where the regular web development tools come into play such as HTML CSS, JavaScript,.

- There were few safety measures that needed to be taken care of which were that the encryption algorithm being used that is the Caesar Cipher needed to be implemented correctly hence making the process secure and reliable
- It needed to be made sure that there was a scope in order to modify the encryption code in the website in the future so that the problems encountered can be changed and can be made even more secure in the future.

3.3 DESIGN SELECTION AND FLOW

The design selected to be be implemented focused mainly on two concepts one was making the code for the encryption fully secure and reliable making it hard to decrypt and secondly the user interface of the project needed to be highly easy to use so that the only thing the user needed to take care of was the size of key being selected and the text being entered and results could be easily made visible to the user not making the process hard.

3.4 IMPLEMENTATION PLAN / METHODOLOGY

There were mainly two components of the whole project; firstly it was that the code for the encryption algorithm needed to be designed. And needed to be integrated with the HTML page so that the user input can be passed to the code of the encrypter that is the string entered along with the key and the final result could be displayed to the user.

CHAPTER 4: RESULT ANALYSIS AND VALIDATION

The project was developed and implemented successfully using the technologies initially stated that are HTML, CSS and JavaScript. The code for Caesar cipher was constructed using JavaScript. While making the use of HTML and CSS in order to structure and style the project to make it user friendly and attractive so that the user not only uses the project for the sake of it but actually has a good time while using the interface of the project.

4.1 IMPLEMENTATION OF DESIGN

The design was implemented using HTML, CSS and JavaScript. There were mainly three components that needed to be implemented. In order to make the whole project working and useful.

1. **DESIGNING THE ALGORITHM IN ORDER TO ENCRYPT THE USER INPUT :**

A secure algorithm needs to be designed in order to encrypt the data of the user entered in such a way that it is highly secure and takes a lot of time to crack. For this the algorithm implemented was Cesar Cipher in order to encrypt the text entered by the user in such a way so that the key using which the text is to be encrypted was user defined in order to give the user expected results along with making the encryption process more personalized. Along with encryption the decryption algorithm also needed to be generated so that the user is not only able to encrypt the text but is able to do other two things as well firstly is to see if the code is encrypted correctly that is using the decryption functionality and also to decipher any texts received from other sources.

2. **STRUCTURING THE USER INTERFACE**

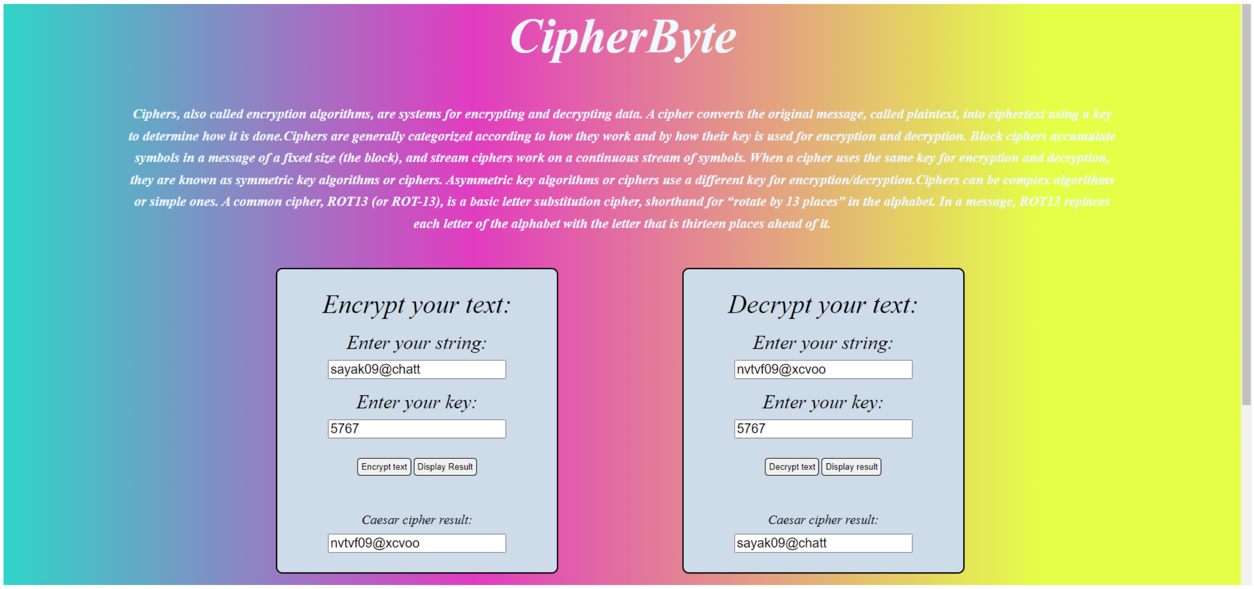
The user The user interface needed to be structured in such a way that information was visible to the user correctly and the user was able to make use of the interface in a circle in such a way that the text that needed to be encrypted was easily input to the website and the website was able to give output to the user and display it on the interface clearly and the user didn't have to make many changes in the already present interface just to view the results

3. **CONNECTING WEBPAGE WITH THE CODE TO BE IMPLEMENTED:**

after coding the Encryption Algorithm that needed to be embedded into the HTML page in such a way that the user input could be input to the code generated for encryption and the key to enter key that the user in wanted to encrypt was also given by the user itself and that he was passed to the court that was made to encrypt so that the text entered by the user would be encrypted using that key. the output of the code needed to be structured in such a way that the output would be displayed on the HTML page easily.

4.2 RESULT OF THE IMPLEMENTATION

After implementing all the languages and the concepts using HTML and CSS and JavaScript the final product was as follows. majorly having two main components that was the user interface and secondly was the user input that was entered by the user.



CipherByte

Ciphers, also called encryption algorithms, are systems for encrypting and decrypting data. A cipher converts the original message, called plaintext, into ciphertext using a key to determine how it is done.Ciphers are generally categorized according to how they work and by how their key is used for encryption and decryption. Block ciphers accumulate symbols in a message of a fixed size (the block), and stream ciphers work on a continuous stream of symbols. When a cipher uses the same key for encryption and decryption, they are known as symmetric key algorithms or ciphers. Asymmetric key algorithms or ciphers use a different key for encryption/decryption.Ciphers can be complex algorithms or simple ones. A common cipher, ROT13 (or ROT-13), is a basic letter substitution cipher, shorthand for "rotate by 13 places" in the alphabet. In a message, ROT13 replaces each letter of the alphabet with the letter that is thirteen places ahead of it.

Encrypt your text:

Enter your string: sayak09@chatt

Enter your key: 5767

Caesar cipher result: nvtvf09@xcvoo

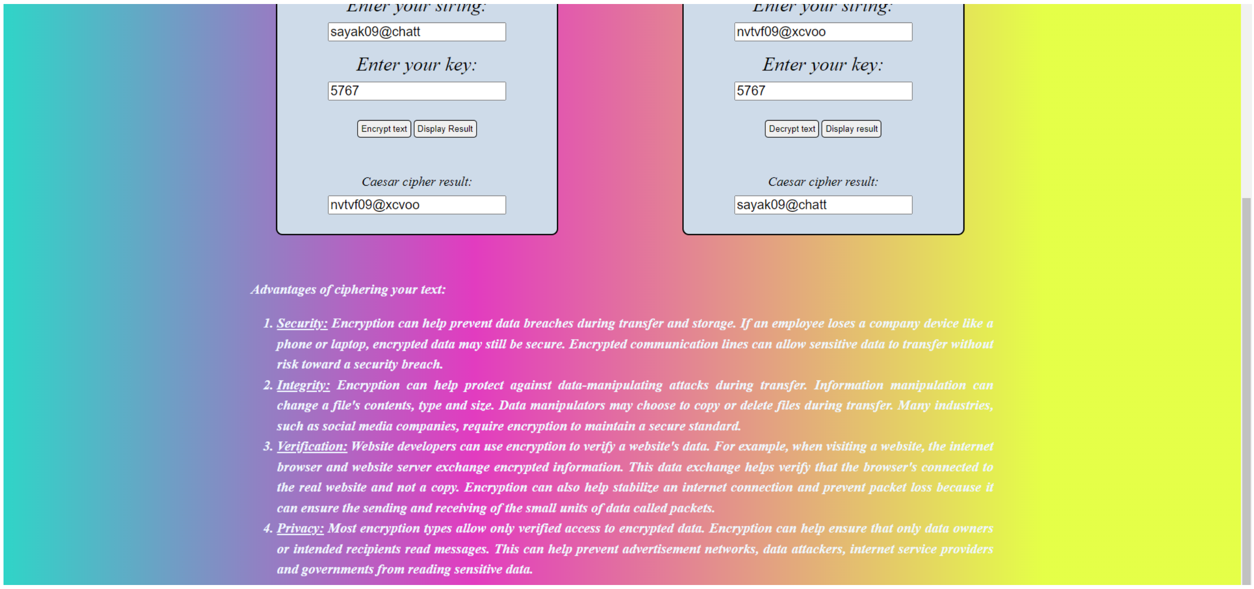
Decrypt your text:

Enter your string: nvtvf09@xcvoo

Enter your key: 5767

Caesar cipher result: sayak09@chatt

Fig 4.1 Graphical user interface



Enter your string: sayak09@chatt

Enter your key: 5767

Caesar cipher result: nvtvf09@xcvoo

Enter your string: nvtvf09@xcvoo

Enter your key: 5767

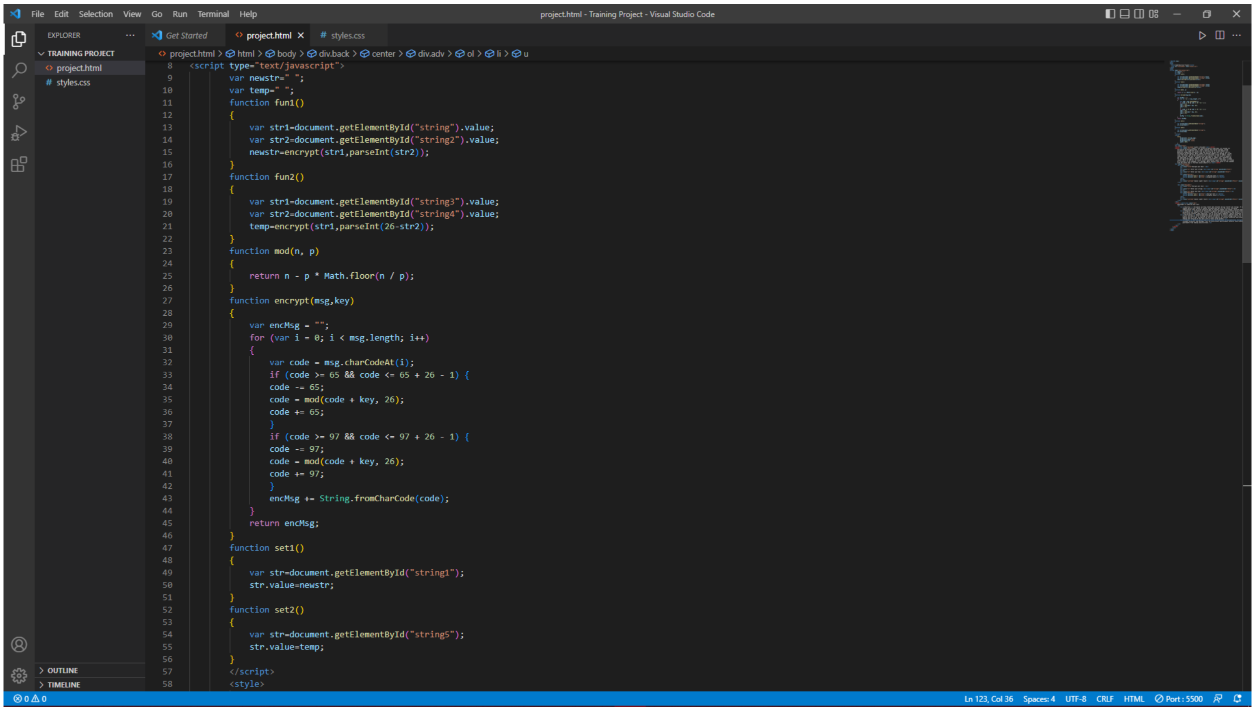
Caesar cipher result: sayak09@chatt

Advantages of ciphering your text:

1. *Security: Encryption can help prevent data breaches during transfer and storage. If an employee loses a company device like a phone or laptop, encrypted data may still be secure. Encrypted communication lines can allow sensitive data to transfer without risk toward a security breach.*
2. *Integrity: Encryption can help protect against data-manipulating attacks during transfer. Information manipulation can change a file's contents, type and size. Data manipulators may choose to copy or delete files during transfer. Many industries, such as social media companies, require encryption to maintain a secure standard.*
3. *Verification: Website developers can use encryption to verify a website's data. For example, when visiting a website, the internet browser and website server exchange encrypted information. This data exchange helps verify that the browser's connected to the real website and not a copy. Encryption can also help stabilize an internet connection and prevent packet loss because it can ensure the sending and receiving of the small units of data called packets.*
4. *Privacy: Most encryption types allow only verified access to encrypted data. Encryption can help ensure that only data owners or intended recipients read messages. This can help prevent advertisement networks, data attackers, internet service providers and governments from reading sensitive data.*

Fig 4.2 Graphical user interface

The following is a screenshot of the code that was implemented for the project.


File Edit Selection View Go Run Terminal Help
project.html - Training Project - Visual Studio Code
EXPLORER
TRAINING PROJECT
project.html
styles.css
Get Started
project.html
styles.css
project.html > html > body > div.back > center > div.adv > ol > li > u
OUTLINE
TIMELINE
Ln 123, Col 36 Spaces: 4 UTF-8 CRLF HTML Port : 5500

```
<script type="text/javascript">
        var newstr=" ";
        var temp=" ";
        function fun1()
        {
            var str1=document.getElementById("string").value;
            var str2=document.getElementById("string2").value;
            newstr=encrypt(str1,parseInt(str2));
        }
        function fun2()
        {
            var str1=document.getElementById("string3").value;
            var str2=document.getElementById("string4").value;
            temp=encrypt(str1,parseInt(26-str2));
        }
        function mod(n, p)
        {
            return n - p * Math.floor(n / p);
        }
        function encrypt(msg,key)
        {
            var encMsg = "";
            for (var i = 0; i < msg.length; i++)
            {
                var code = msg.charCodeAt(i);
                if (code >= 65 && code <= 65 + 26 - 1) {
                code -= 65;
                code = mod(code + key, 26);
                code += 65;
                }
                if (code >= 97 && code <= 97 + 26 - 1) {
                code -= 97;
                code = mod(code + key, 26);
                code += 97;
                }
                encMsg += String.fromCharCode(code);
            }
            return encMsg;
        }
        function set1()
        {
            var str=document.getElementById("string1");
            str.value=newstr;
        }
        function set2()
        {
            var str=document.getElementById("string5");
            str.value=temp;
        }
        </script>
        <style>
```

Fig 4.3 Code of the project

4.3 DATA VALIDATION

the data entered by the users into the Encryption Algorithm and the output received by the user needed to match what the code was actually meant to do this could be checked using the d ciphertext a function of the project. decrypted was the correct result that was received master initial into input that and that was to be decrypted. and the encryption of the project could be checked during the decryption functionality that is a the text that was encrypted by the user that would be deciphered right at that moment and can be seen if the text that was this iPad and the text that was initially in input to the website for encryption actually map or not

CHAPTER 5: CONCLUSION AND FUTURE WORK

After having an indepth look about the concept of cyber security it can be concluded that cybersecurity's importance is on the rise. Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow. Data leaks that could result in identity theft are now publicly posted on social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive. The fact of the matter is whether you are an individual, small business, or large multinational, you rely on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones, and the Internet of Things (IoT) and we have a myriad of potential security vulnerabilities that didn't exist a few decades ago. We need to understand the difference between cybersecurity and information security, even though the skillsets are becoming more similar.

5.1 EXPECTED RESULTS

This project is aimed to provide a more secure and simple way of communication between two individuals. It is meant to be used to keep the private information safe while being sent over any application. It is expected to be used in different projects where there is a need to ask for important information from the user and that needs to be sent over a channel or is to be stored in the database, having a key that is very hard to figure out or requires a huge amount of time to decrypt can prove to be a highly secure way of sending and storing information hence making it a useful tool both at individual as well as organization level. This project along with being a stand alone project has a lot of scope in being used in authentication systems and as the number of websites on the internet are increasing therefore the need for login/authentication systems will also increase making the project more useful.

5.2 FUTURE SCOPE

The presence of new malware, spyware, ransomware, trojans, and worms grows every day. As more and more systems connect to cyberspace, they become vulnerable to attacks from all corners of the world. Every organization and business needs to protect its assets and data against any such attacks. This increased need unlocks many job prospects for computer engineers looking for jobs in a cutting-edge and fast-growing field of cybersecurity. Ethical hacking is an example of an excellent opportunity to improve the security of the network and systems, specifically by testing for such vulnerabilities.By learning ethical hacking, you can play a vital role in securing the systems and data from threats and attacks. As an ethical hacker, we can:

- Conduct investigations and analyses of the target systems to identify any security or system vulnerabilities from the hacker's point of view and suggest a remedy
- Help implement a state-of-the-art network that can withstand security breaches
- Help government agencies in safeguarding a nation's infrastructure from extremists
- Protect consumer data and information by implementing best in class security practices, thereby maintaining trust and confidence
- Do a controlled assessment on enterprise networks and systems by mimicking a real-time attack; identify and report flaws to better prepare for impending malicious hacker attacks

Along with cybersecurity having a lot of scope in the future, this project can also stand the test of time with modifications being done according to the changing requirements. These changes can be made in the encryption algorithm being used in order to make it more complex hence increasing the level of difficulty the attacker would have to face to try to crack it without having the actual key needed to decrypt the code hence fully solving the actual aim of the project.

5.3 REFERENCES

1. https://owasp.org/
2. https://www.synopsys.com/glossary/what-is-ethical-hacking.html
3. https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ethical-hacking
4. https://intellipaat.com/blog/vulnerability-in-cyber-security/
5. https://trainings.internshala.com/
6. https://trainings.internshala.com/progress/home/hacking/
7. https://portswigger.net/web-security/access-control/idor
8. https://www.fortinet.com/resources/cyberglossary/brute-force-attack
9. https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Securit
10. "Application Vulnerabilities Trends Report: 2014," Cenzic Inc., Campbell, CA, 2014.

11. K. S. Alghathbar, M. Mahmud and H. Ullah "Most known vulnerabilities in Saudi Arabian web servers," in Internet, 2008. ICI 2008. 4th IEEE/IFIP, Tashkent, 2008 © IEEE. doi: 10.1109/CANET.2008.4655317.
12. [5] J. J. Zhao and S. Y. Zhao, "Opportunities and threats: A security assessment of state e-government websites," in Government Information Quarterly 27, 2010, pp. 49–56.