CipherByte

A training project

Name: Sayak Chatterjee

UID: 20BCS1452

Section: 20BCS_WM-706A

Training and Learnings

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.

The concepts and tools taught:

1. *Basics of Security and Computer Networking*
2. *Information gathering and web development*
3. *Introduction to Web VAPT, OWASP and SQL*
4. *Advanced Web Application attacks*
5. *Identifying security misconfigurations and exploiting outdated web applications*
6. *Automating VAPT*
7. *Documentation and Reporting Vulnerabilities*

Encrypt-Decrypt Concept Generation

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext.There can be different algorithms that can be used in order to cipher the text which are already defined such as ***Caesar Cipher*** or developer defined algorithms. The encryption algorithm used in the project is Caesar 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. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Implementation

The technologies used in order to implement the project are: HTML, CSS, JavaScript

Three main components

1. ***Design Algorithm to process input:***

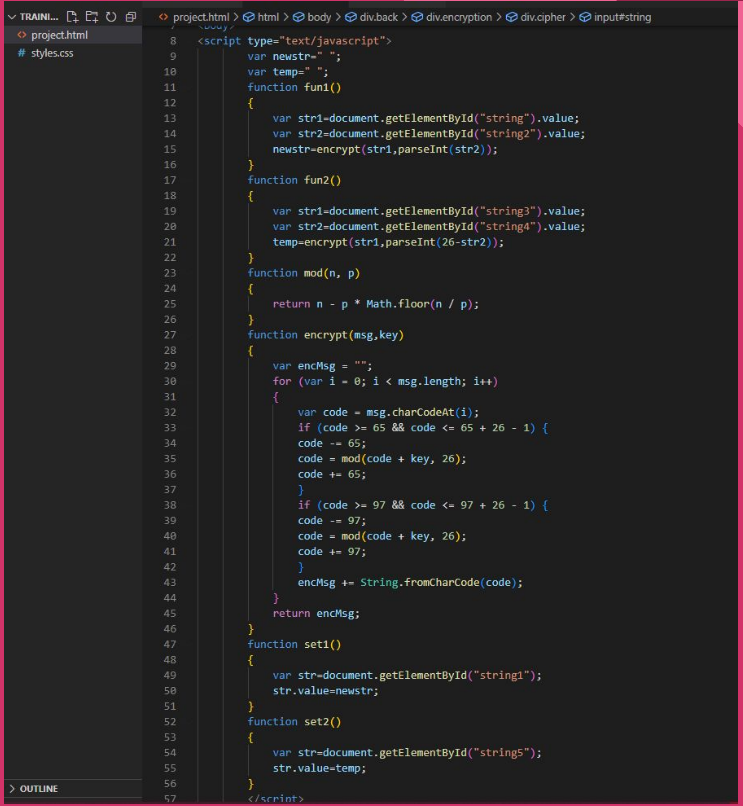
A secure algorithm needs to be designed in JavaScript in order to encrypt the data of the user entered in such a way that it is highly secure and takes a lot of time to crack.

2. ***Structuring 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 interface was user friendly

3. ***Connecting webpage with the code to be implemented:***

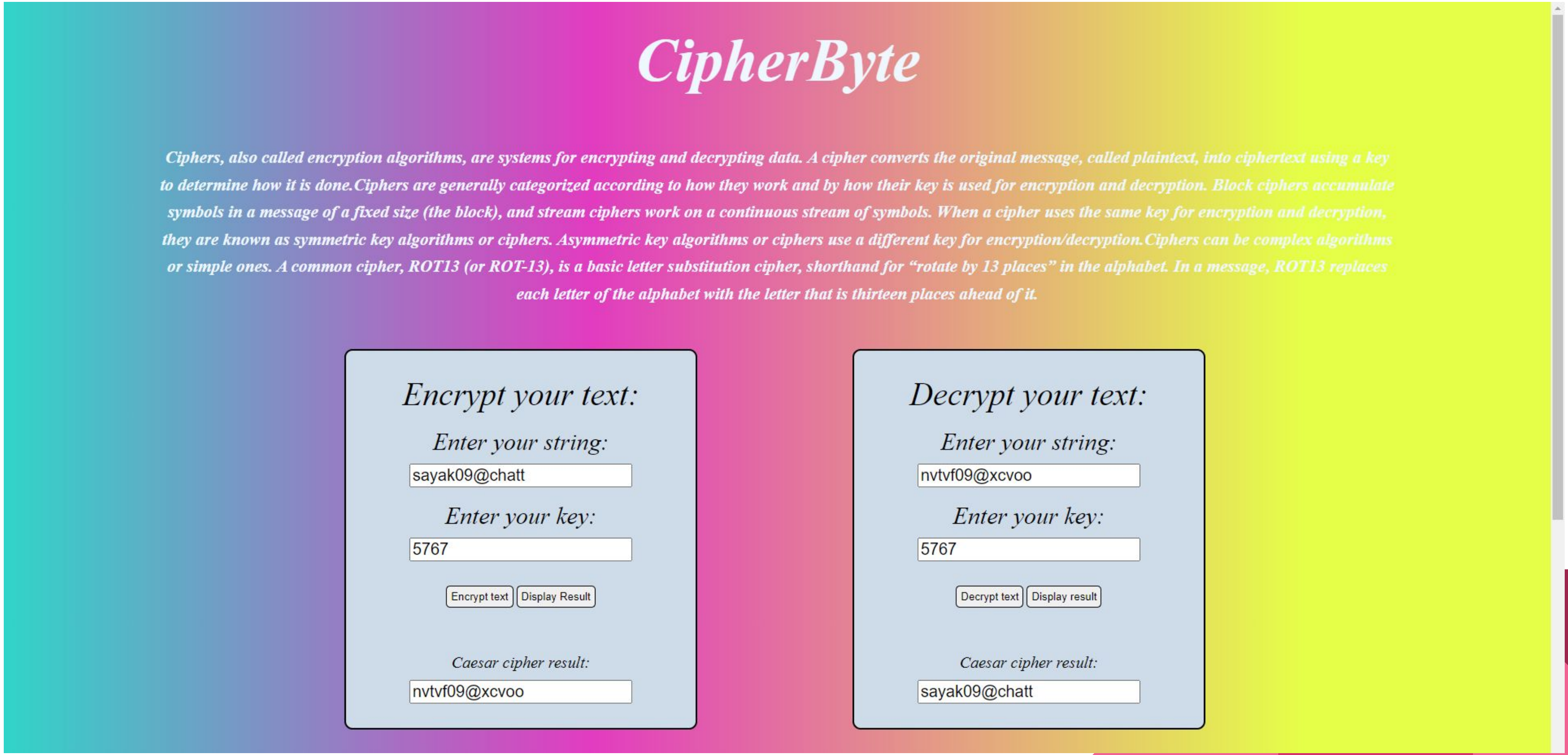
After coding the Encryption Algorithm that needed to be embedded into the HTML page in such a way that the user input could be input to the code and that the output would be displayed on the HTML page easily.



TRAINI...
project.html
styles.css
OUTLINE
project.html > html > body > div.back > div.encryption > div.cipher > input#string

```
<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>
```

Final Result



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

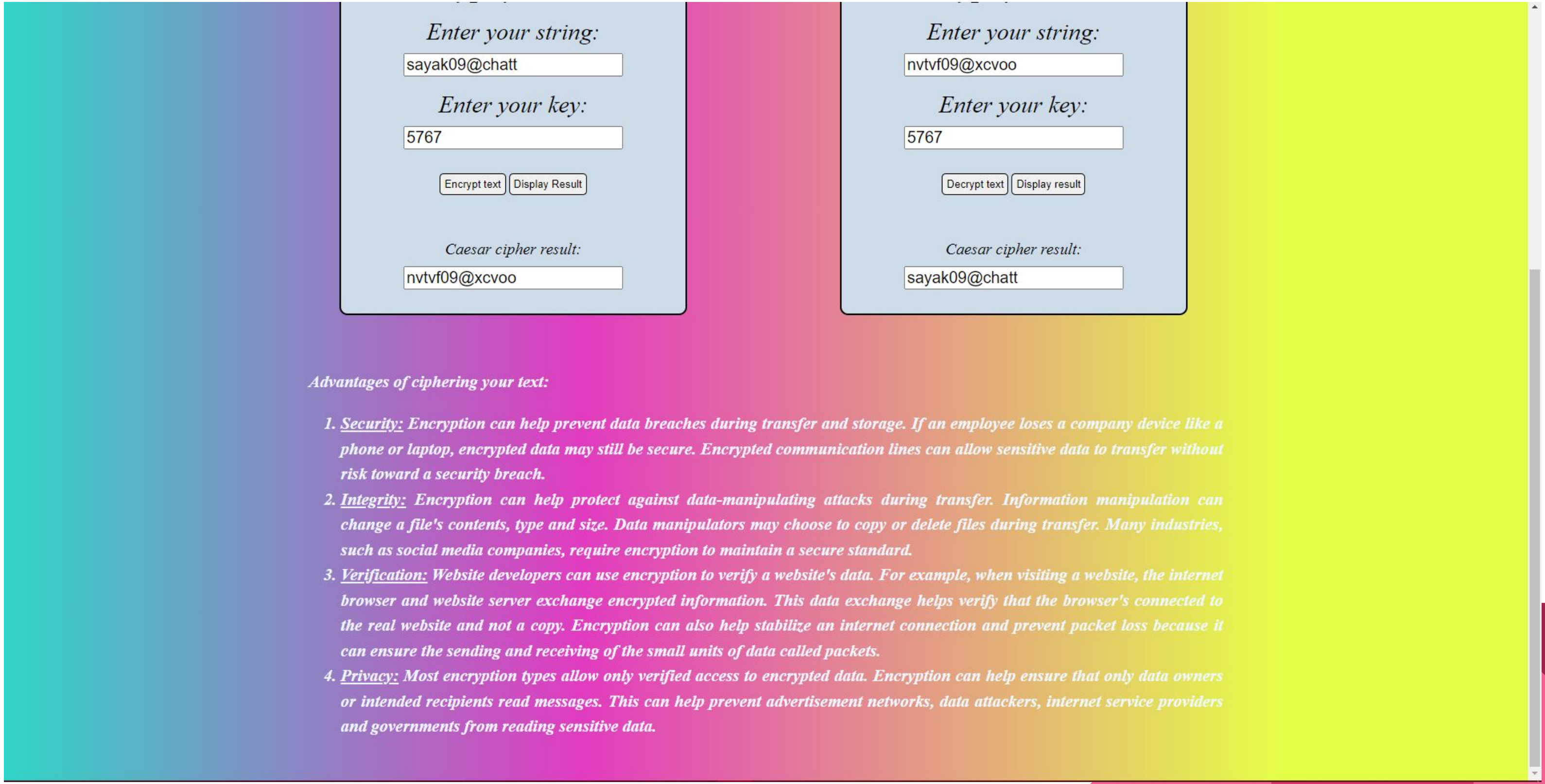
Enter your key:

5767

Caesar cipher result:

sayak09@chatt

Final Result



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.*

Advantages of the project

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.

Future Scope

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 that is able to main high level security along with reliability of the user as well as any other product it is a part of.

Thankyou