WEB APPLICATION FOR CUSTOMIZED MESSAGE ENCRYPTION

ISS PROJECT

A PROJECT REPORT

Submitted by

Aditya Kishan 17MIS7027

Sampath 17MIS7119

Under the Guidance of

Dr.S.Sudhakar Ilango

Associate Professor, CSE,

VIT-AP

TABLE OF CONTENTS

Chapter -1

Introduction

While most of the conversation in businesses and internal organization is carried over instant messaging platforms, securing the interaction is the major priority for businesses and companies to stay away from losing millions of dollars every year.

Communication is the lifeline for businesses. In the present-day scenario, a vast amount of business data and personal information are managed online and stored on cloud servers. Encrypted communication becomes imperative to protect information and data that you send and receive from third parties and service providers. Sensitive and business-affecting information needs to be exchanged on secure chat platforms to achieve the objective of secrecy and security.

Through our proposed mini-project we aim to create a simple web application which would support “customized message encryption and transfer”.

Since this is the pilot version of our mini project, we thought of including basic encryption methods in the starting.(like Caeser Cipher , Rail-fence cipher, Transposition technique etc).We hope that after further inclusion of highly secure encryption methods in the application, it can be used for military/Secret/Undercover services.

Chapter -2

Background Study

Though our project idea is completely niche and it serves only a specific type of organization, we were keen to study about various features, encryption methods used ,specific domain and market value of exisiting secure chat applications in the market.

Following are some of the few market leaders:

- **KryptoChat Secure Messaging Platform**

  KryptoChat is a secure messaging application based on military-grade encryption developed by Kryptotel.

  https://www.kryptochat.com/

- **TeamWire**

  Teamwire is an enterprise messaging company from Germany. The headquarters are in Munich and the company was founded in 2010.

  https://www.teamwire.eu/

According to a new market research report "Encryption Software Market by Component (Software and Services), Application (Disk Encryption, File/Folder Encryption, Communication Encryption, Cloud Encryption), Deployment Mode, Enterprise Size, Vertical, and Region - Global Forecast to 2024", published by MarketsandMarkets™, the global Encryption Software Market size is expected to grow from USD 7.5 billion in 2019 to USD 16.5 billion by 2024, at a Compound Annual Growth Rate (CAGR) of 17.0% during the forecast period.

Chapter -3

Problem Definition

We know that for decades programmers and information security experts have been striving hard to create highly secure message encryption mechanisms so that it cannot be deciphered easily by phisers and hackers. We need to accept the fact that even their methods of phising and snooping has evolved with time. Gone are the days when they used brute force method to decipher the encrypted data. They always look for patterns and periodicity in the data and once they know the encryption method used, the decryption time decreases drastically.
If worlds richest person’s phone can be hacked what about the common folks!!

There are plethora of web-based message application services available on internet. But each of them lack in one or more areas that we offer. Some of them are too costly to be afforded, while others offer a very few services. There are a few free secure chat applications, but the UI is so cluttered with irrelevant ads that client would not like to visit it again.

Also there isn’t any application till now which has used random encryption method that too with random keys every time.

Also we are aware that the problem is niche and it will serve a small chunk of the large and exponentially growing chat application market.

Chapter -4

Objective

So following are some of the objectives that we aim to achieve through our project "**Web Application For Customized Message Encryption":-**

- Clean and clutter free UI
- Authenticated access to the platform(Only registered users allowed)
- Provide at-least two encryption method to toggle while chatting. Since its our pilot project we are using simple encryption methods like **Caeser Cipher and Rail-fence cipher**.
- Inclusion of Tawk.to chat widget in the application so that **"Informers"** can chat with **"Admin".** In case the admin receives lots of chat requests then there is an option to add additional agents to manage and accept those chat requests. Apart from this tawk.to also provides information like name,location and email-id of the informer to the admin.
- Profile edit option for all types of informers wherein they can update, add information or delete their account.
- To provide secure logout.All sessions specific to the logged-in user is destroyed.

Chapter -5

Methodology/Procedure

So basically this application is supposed to be used by a single organization(most preferably by an organization which deals with exchange of "private" and "sensitive" information).There are two types of participants who will be using the application:

- Informers (the one who carries sensitive information)
- Admin (the one who gives instructions to informers and seeks information)

The informer will initiate the chat by logging into his own account. The Admin will get the chat request on his **"tawk.to"** website/mobile app and can choose to join the chat. All the details of the informer like name, location, email-id will be visible to admin. In case the admin is busy and wasn't able to attend the chat request he can transfer it to other chat agent who is free. Alternatively he can appoint another person as an admin by inviting him through e-mail.

In order to create an ambiguity and confusion about the encryption method used to encrypt the message(for phisers), we will use multiple encryption method randomly selected by users. At the end of each encrypted message a "method number" and a "key" corresponding to a particular encryption method should be entered. On receiving the encrypted message, the receiver can decipher it using the corresponding decryption method. The chat can go on like that.The sender must have registered before accessing the service. For message exchange(after manual encryption) we will be using third party messaging platform "Tawk.to".

Chapter -6

Results and Discussion

After completing the project we did some testing and trials. Following are some of the findings and progress we observed:

- Clean and clutter free UI experience feedback from the volunteers who tried the applications. This fulfills our first objective,
- Failed attempt to access the application without proper authentication.(please see the corresponding screenshot in the screenshot section of the report)
- Users faced slight difficulty in toggling between the two encryption methods and it was a bit time consuming according to them. We have discussed in detail about it in next section.
- However test users liked easy and clutter free profile edit option

Chapter -7

Conclusion and Future Scope

Although almost every requirement stated in the SRS(requirements) document has been covered, there is still a lot of scope for improvement, accuracy, reliability and ease of use.

As of now we have included only two encryption options(Caeser cipher and Rail-Fence Cipher). But two provide better security we need to include more and complex methods in our future releases. Also some of the test users complained about difficulty in toggling between the two methods for encryption and decryption of chats. That’s why we are planning to automate the process of random selection of methods and key.

Presently anyone outside of the specific organisation can also register and create an account. We are considering it as a major security issue. We are planning to accept only those accounts whose e-mail address corresponds to that particular organisation. In this way outsiders won’t be allowed to create an account.

References (Sample)

1. [1] *Fatal error: Uncaught mysqli_sql_exception:" when inserting into database with mysqli_query [duplicate]* - https://stackoverflow.com/questions/48047137/fatal-error-uncaught-mysqli-sql-exception-when-inserting-into-database-with
2. [2] *How to connect HTML Register Form to MySQL Database with PHP* - https://www.youtube.com/watch?v=qm4Eih_2p-M
3. [3] *How to retrieve data from a checkbox using PHP* - http://www.learningaboutelectronics.com/Articles/How-to-retrieve-data-from-a-check-box-with-PHP.php
4. [4] *mysql how to fix Access denied for user 'root'@'localhost'* - https://superuser.com/questions/603026/mysql-how-to-fix-access-denied-for-user-rootlocalhost?rq=1
5. [5*] php mysqli_connect: authentication method unknown to the client [caching_sha2_password]* - https://stackoverflow.com/questions/50026939/php-mysqli-connect-authentication-method-unknown-to-the-client-caching-sha2-pa
6. [6] *Relation view missing in MYPHP* - https://www.youtube.com/watch?v=86H6b3SuaEk
7. [7]https://stackoverflow.com/questions/43935255/regular-expression-for-name-with-spaces-allowed-in-between-the-text-and-avoid-sp
8. [8] (*when my nav-bar was overlapping with other ui element)* https://www.freecodecamp.org/forum/t/solved-why-is-my-navbar-covering-next-section-container/97897/4
9. [9] (*for hosting website)* https://in.000webhost.com/
10. [10]https://www.w3schools.com/howto/howto_css_image_overlay.asp

Appendix – A

Coding

Caeser cipher code (embedded in caeser.php)

```
    <div id="wrap">
        <legend>Caeser Cipher Encryption/Decryption</legend>
        <script>
var mode = "ceaser";
var shift;
function encrypt() {
var a,b,result="";
text=String(document.getElementById("first").value);
shift=Number(document.getElementById("second").value);




    if (mode == "ceaser"){

        //loop through each caharacter in the text
        for (var i = 0; i < text.length; i++) {

             //get the character code of each letter
            var c = text.charCodeAt(i);

            // handle uppercase letters
```

```
      if(c >= 65 && c <=  90) {
        result += String.fromCharCode((c - 65 + shift) % 26 + 65);

      // handle lowercase letters
      }else if(c >= 97 && c <= 122){
        result += String.fromCharCode((c - 97 + shift) % 26 + 97);

      // its not a letter, let it through
      }else {
        result += text.charAt(i);
      }
    }
  }
  document.getElementById("answer").value= String(result);
  return result;
}

function decrypt(){

  var a,b,result="";
  text=String(document.getElementById("first").value);
  shift=Number(document.getElementById("second").value);
  shift = (26 - shift) % 26;


  if (mode == "ceaser"){
    //loop through each caharacter in the text
    for (var i = 0; i < text.length; i++) {

        //get the character code of each letter
      var c = text.charCodeAt(i);

      // handle uppercase letters
      if(c >= 65 && c <=  90) {
        result += String.fromCharCode((c - 65 + shift) % 26 + 65);

      // handle lowercase letters
      }else if(c >= 97 && c <= 122){
        result += String.fromCharCode((c - 97 + shift) % 26 + 97);

      // its not a letter, let it through
      }else {
        result += text.charAt(i);
      }
    }
  }


  document.getElementById("answer2").value= String(result);
  return result;
}
```

```
</script>

Enter the Plain/Cipher text :  <input id="first" type="text"
STYLE="color: #FFFFFF; font-family: Verdana; font-weight: bold;
font-size: 12px; background-color: #72A4D2;" size="10"
maxlength="90"><br/>

Enter the Shift key: <br/>

<input id="second" type="text" STYLE="color: #FFFFFF; font-family:
Verdana; font-weight: bold; font-size: 12px; background-color:
#72A4D2;" size="10" maxlength="30"> <br/>

<button style="background-color:red;"
onclick="encrypt()">Encrypt</button>

<input id="answer" type="text" STYLE="color: #FFFFFF; font-family:
Verdana; font-weight: bold; font-size: 12px; background-color:
#72A4D2;" size="10" maxlength="90"> <br/>

<button style="background-color:green;"
onclick="decrypt()">Decrypt</button>

<input id="answer2" type="text" STYLE="color: #FFFFFF; font-family:
Verdana; font-weight: bold; font-size: 12px; background-color:
#72A4D2;" size="10" maxlength="90">






        </div><!--End of wrap-->
```

Rail-fence cipher code (embedded in RF_cipher.php)

```
<div id="wrap">
    <legend>Rail-Fence Cipher Encryption/Decryption</legend>

     <script type="text/javascript">
function Encrypt() {
  plaintext = document.getElementById("p").value.toLowerCase().replace(/[^a-z]/g, " ");
  if(plaintext.length < 1){ alert("please enter some plaintext"); return; }
  var key = parseInt(document.getElementById("key").value);
  if(key > Math.floor(2*(plaintext.length-1))){ alert("key is too large for the plaintext length."); return; }
  ciphertext = "";
  for(line=0; line<key-1; line++){
    skip=2*(key-line-1);   j=0;
     for(i=line; i<plaintext.length;){
       ciphertext += plaintext.charAt(i);
       if((line==0) || (j%2 == 0)) i+=skip;
      else i+=2*(key-1) - skip;
      j++;
     }
  }
  for(i=line; i<plaintext.length; i+=2*(key-1)) ciphertext += plaintext.charAt(i);
```

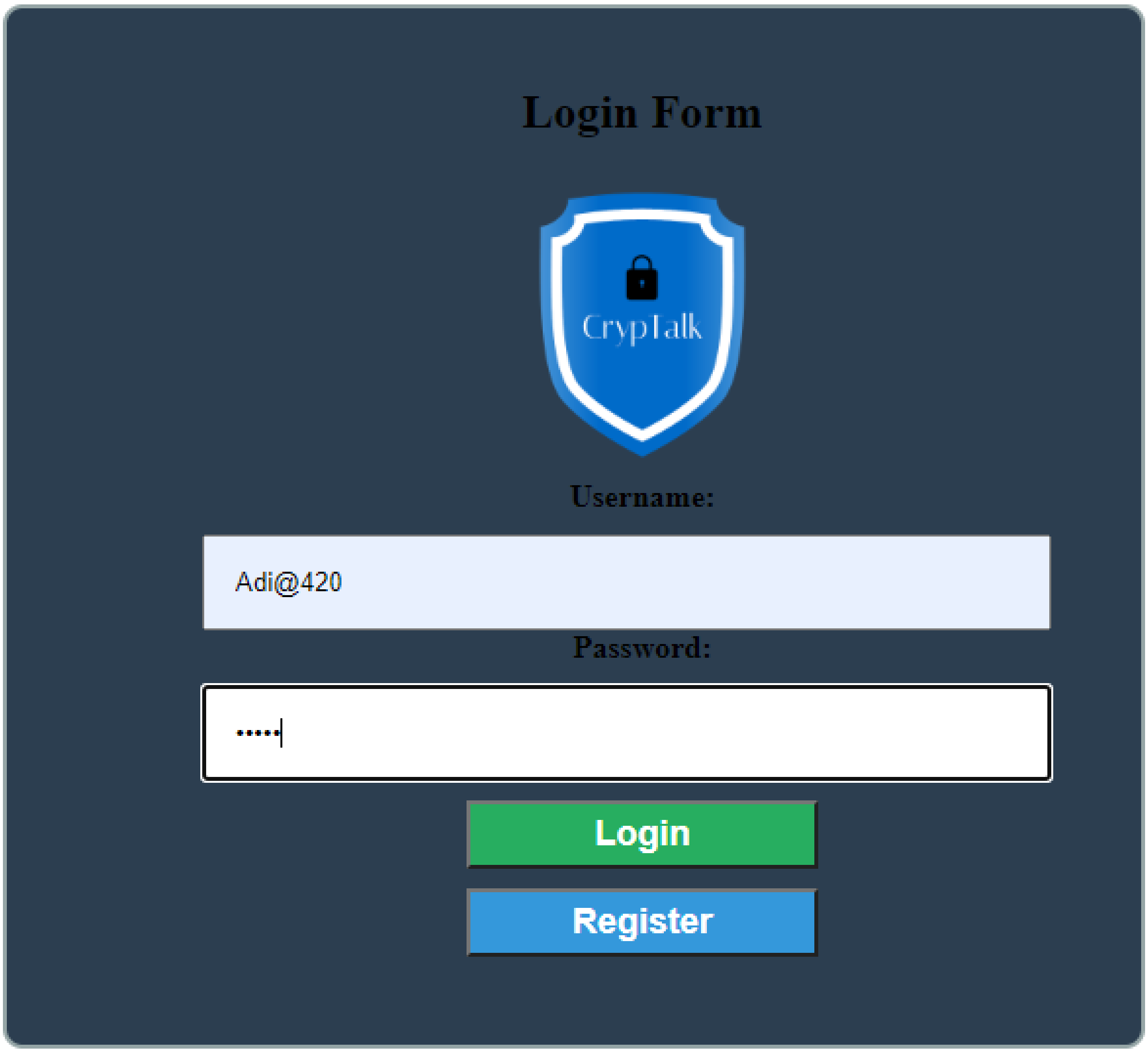
```
   document.getElementById("c").value = ciphertext;
}


function Decrypt(f) {
   ciphertext = document.getElementById("c").value.toLowerCase().replace(/[^a-z]/g, "
");
   if(ciphertext.length < 1){ alert("please enter some ciphertext (letters only)"); return; }
   var key = parseInt(document.getElementById("key").value);
   if(key > Math.floor(2*(ciphertext.length-1))){ alert("please enter 1 - 22."); return; }
   pt = new Array(ciphertext.length);   k=0;
   for(line=0; line<key-1; line++){
      skip=2*(key-line-1);  j=0;
       for(i=line; i<ciphertext.length;){
           pt[i] = ciphertext.charAt(k++);
           if((line==0) || (j%2 == 0)) i+=skip;
          else i+=2*(key-1) - skip;
          j++;
       }
   }
   for(i=line; i<ciphertext.length; i+=2*(key-1)) pt[i] = ciphertext.charAt(k++);
   document.getElementById("p").value = pt.join("");
}
</script>
```

```
<h2>Rail Fence Cipher </h2>

<p>Enter the word that you want to ENCRYPT, then put "NUMBER" in a key form to make how many rail you need</p>


Plaintext<BR>

<TEXTAREA id="p" name="p" rows="4" cols="40" style="background-color:#72A4D2;">ISS Project</TEXTAREA>

<P>line  = <INPUT id="key" name="key" size="5" value=" " type="text" style="background-color:#72A4D2;"></P>

<P><INPUT name="btnEn" value=" Encrypt " style="background-color:red;" onclick="Encrypt()" type="button">

<P><INPUT name="btnDe" value=" Decrypt " style="background-color:green;" onclick="Decrypt()" type="button"></P>

<P>Ciphertext<BR><TEXTAREA id="c" name="c" rows="4" cols="40"style="background-color:#72A4D2;"></TEXTAREA> </P>




        </div><!--End of wrap-->
```

Appendix – B

Snap Shot

Login attempt



Login Form

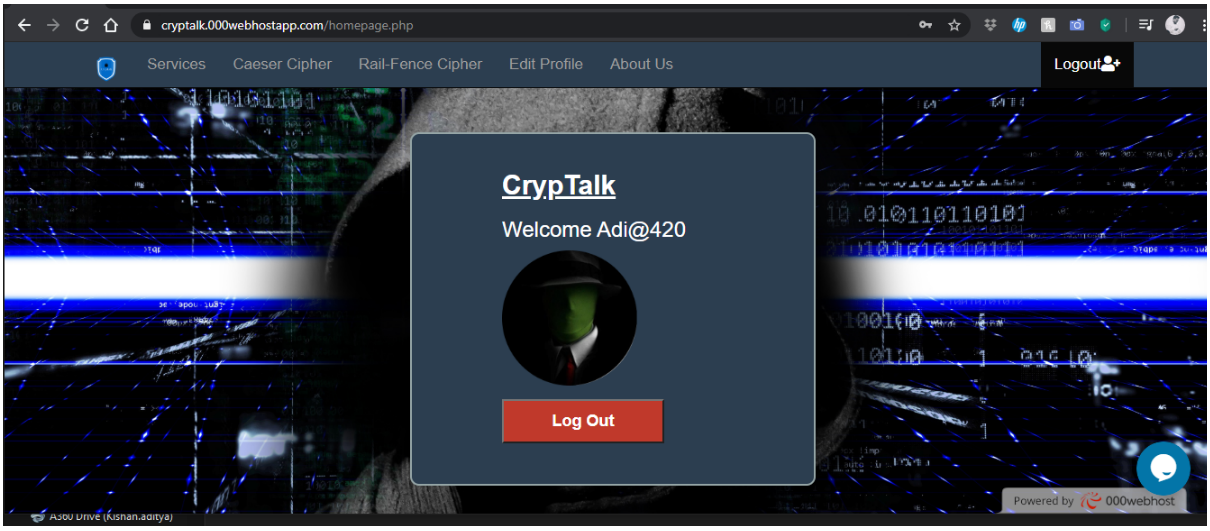
Username:

Adi@420

Password:

•••••

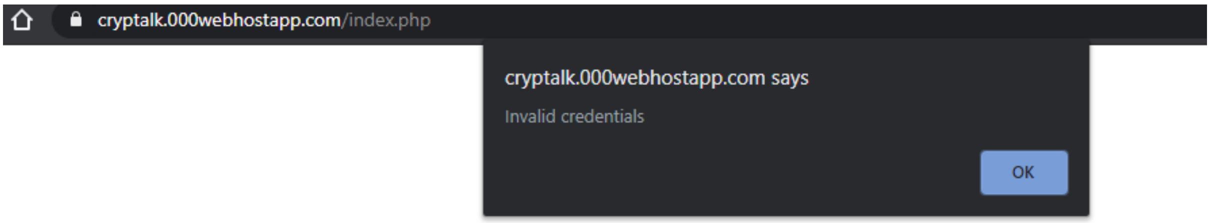
Successful Login



CrypTalk

Welcome Adi@420

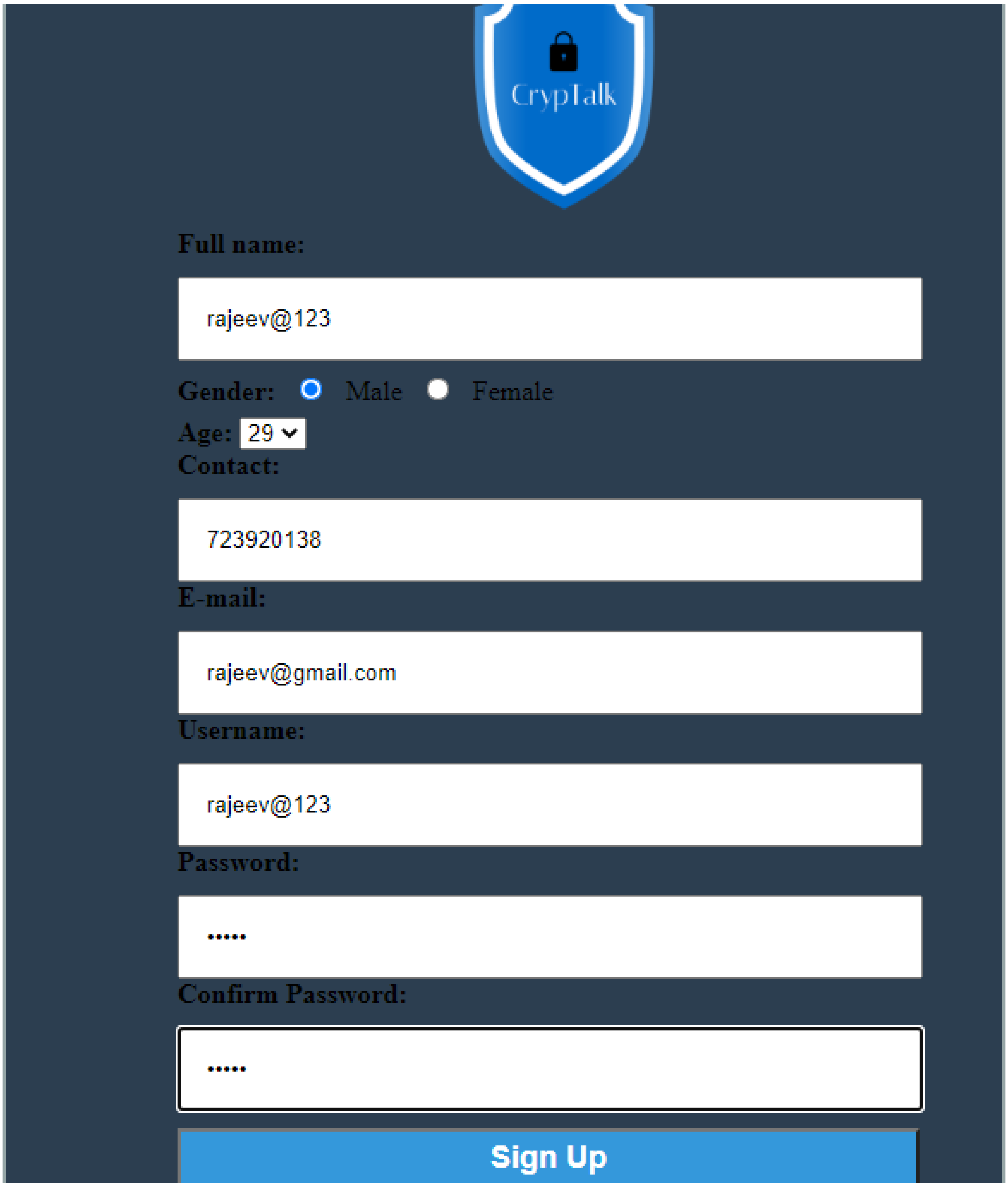
Failed login attempt



cryptalk.000webhostapp.com says

Invalid credentials

Registration Attempt



Full name:

rajeev@123

Gender: ● Male ○ Female

Age: 29

Contact:

723920138

E-mail:

rajeev@gmail.com

Username:

rajeev@123

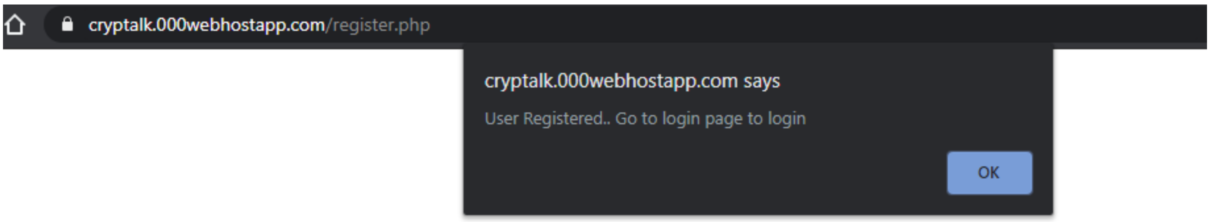
Password:

•••••

Confirm Password:

•••••

Successful registration

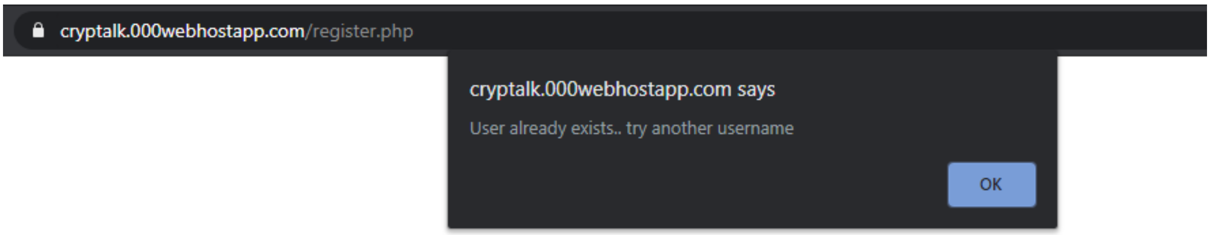


cryptalk.000webhostapp.com/register.php

cryptalk.000webhostapp.com says

User Registered.. Go to login page to login

Failed registration

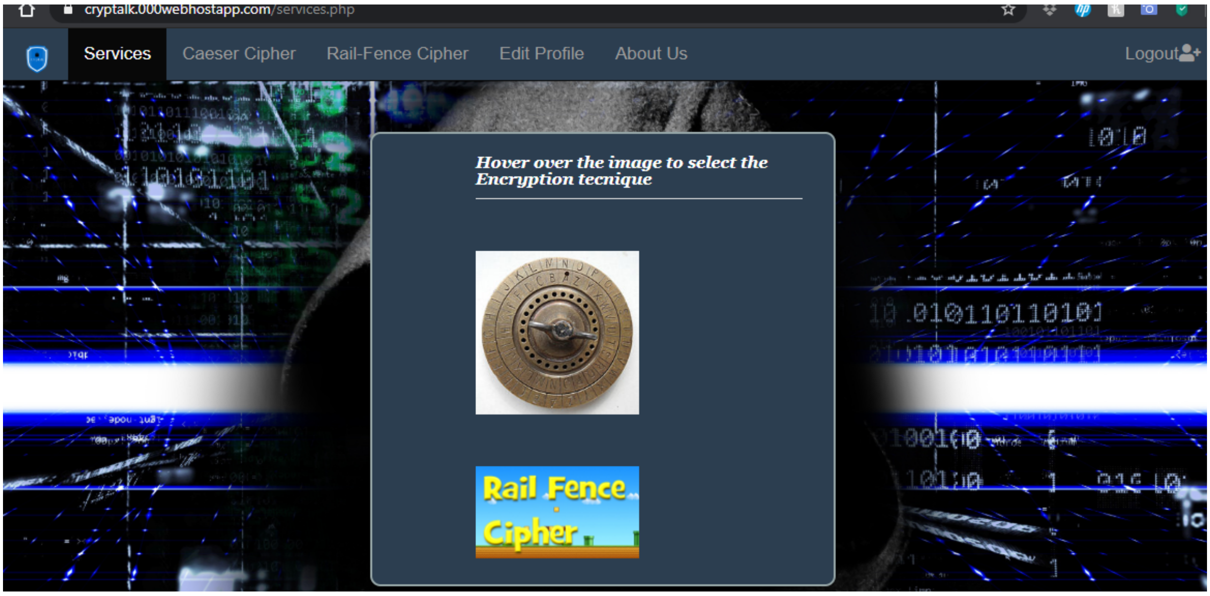


cryptalk.000webhostapp.com/register.php

cryptalk.000webhostapp.com says

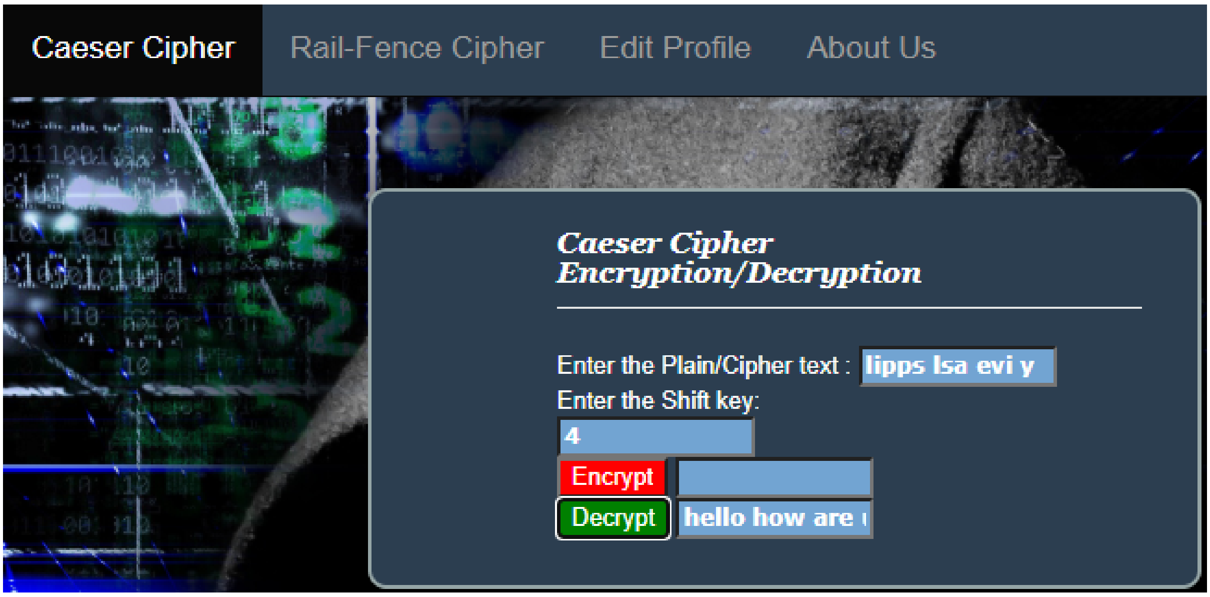
User already exists.. try another username

Services



Hover over the image to select the Encryption tecnique

Caeser cipher



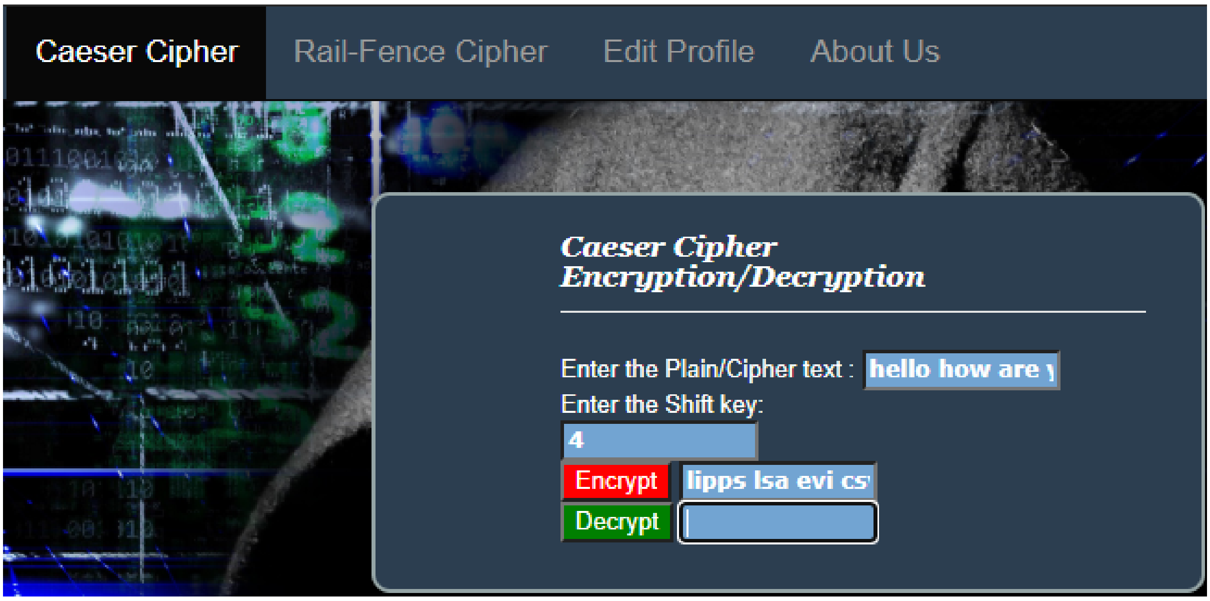
Caeser Cipher Encryption/Decryption

Enter the Plain/Cipher text : lipps lsa evi y

Enter the Shift key:

4

hello how are ι



Caeser Cipher Encryption/Decryption

Enter the Plain/Cipher text : hello how are y

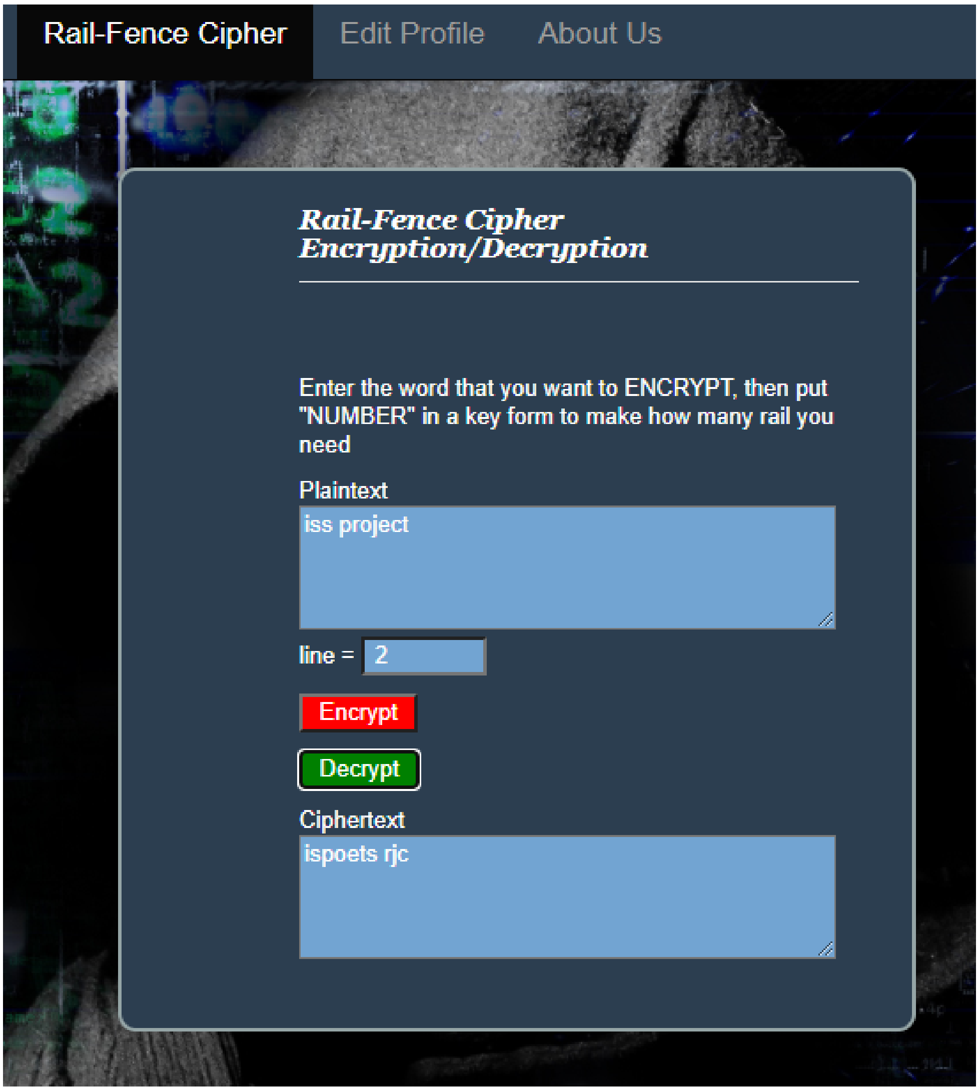
Enter the Shift key:

4

lipps lsa evi cs

Rail-fence cipher(encrypt)

-



Rail-Fence Cipher Encryption/Decryption

Enter the word that you want to ENCRYPT, then put "NUMBER" in a key form to make how many rail you need

Plaintext

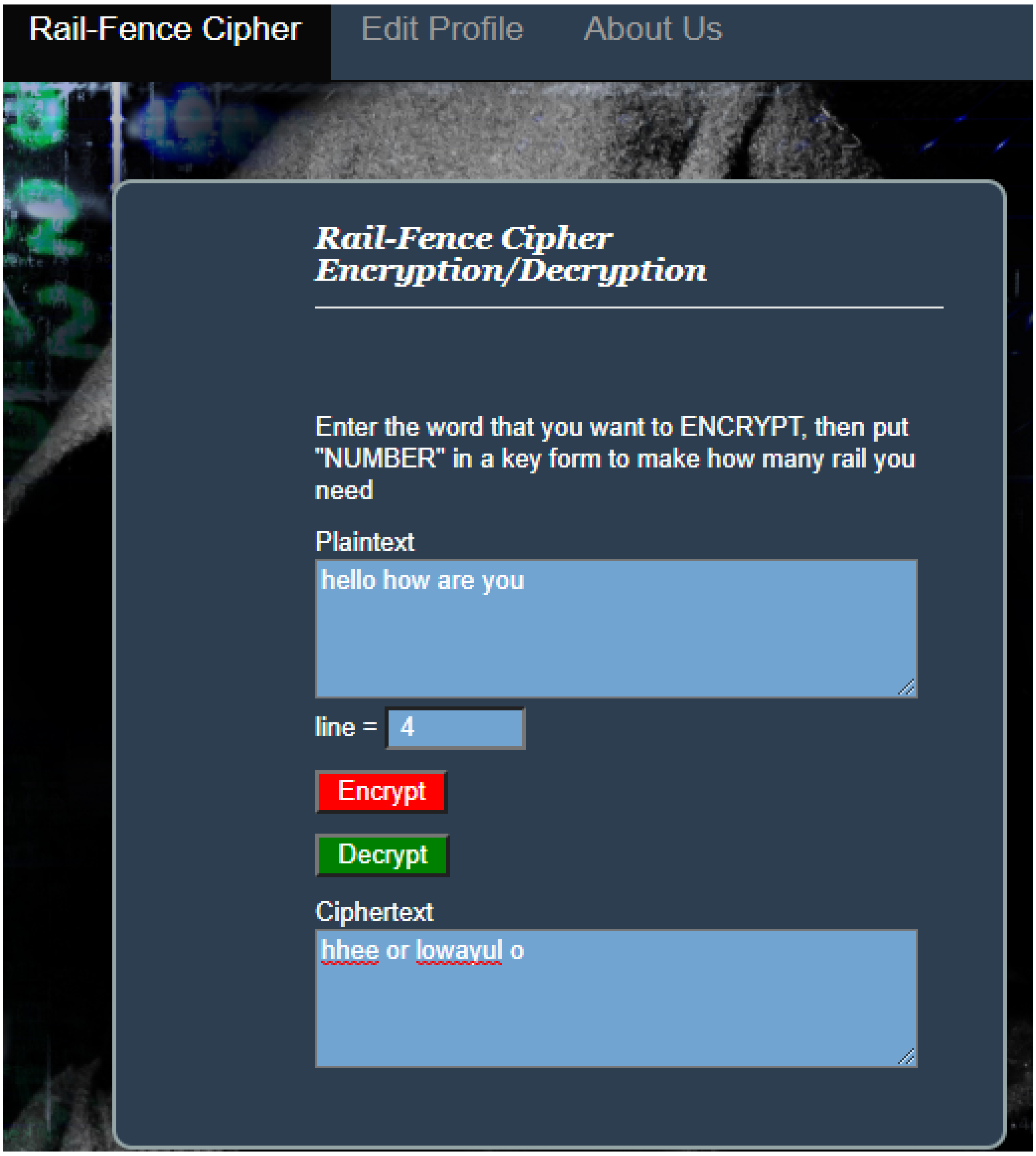
iss project

line = 2

Ciphertext

ispoets rjc

Rail-fence cipher(decrypt)



Rail-Fence Cipher Encryption/Decryption

Enter the word that you want to ENCRYPT, then put "NUMBER" in a key form to make how many rail you need

Plaintext

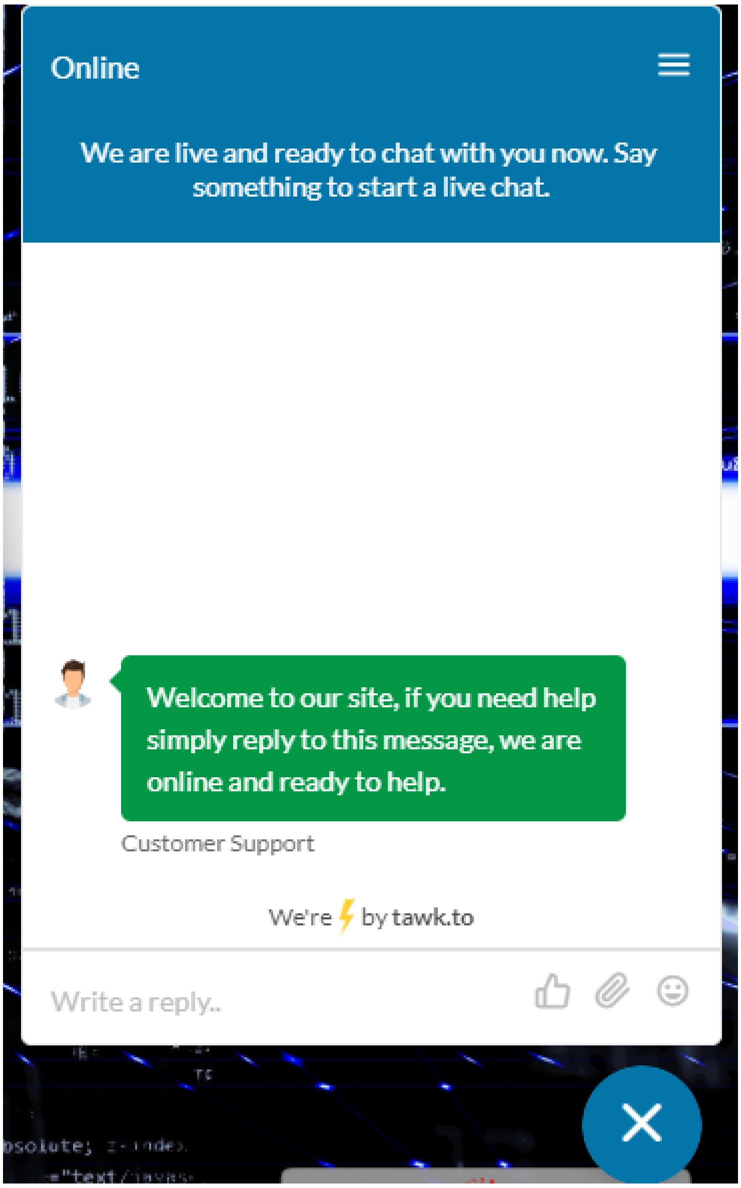
hello how are you

line = 4

Ciphertext

hhee or lowayul o

Twk.to widget

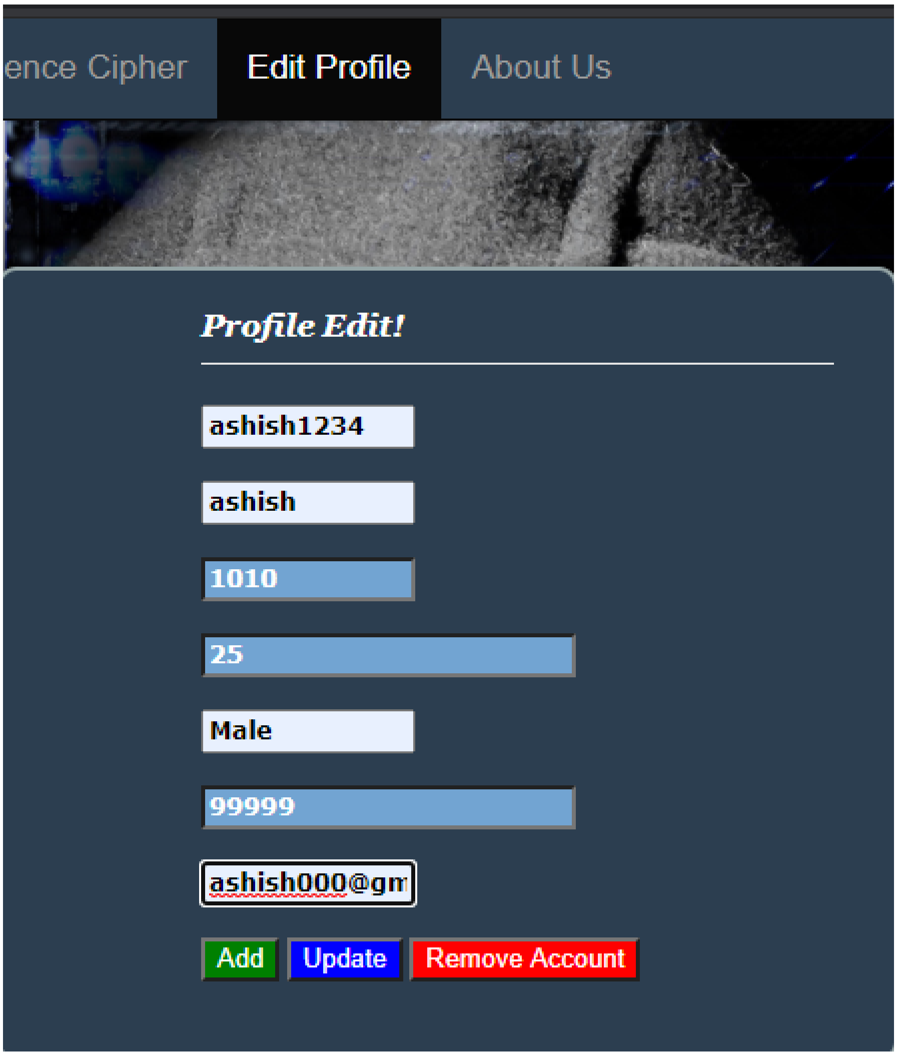


We are live and ready to chat with you now. Say something to start a live chat.

Welcome to our site, if you need help simply reply to this message, we are online and ready to help.

Customer Support

Edit



Profile Edit!

ashish1234

ashish

1010

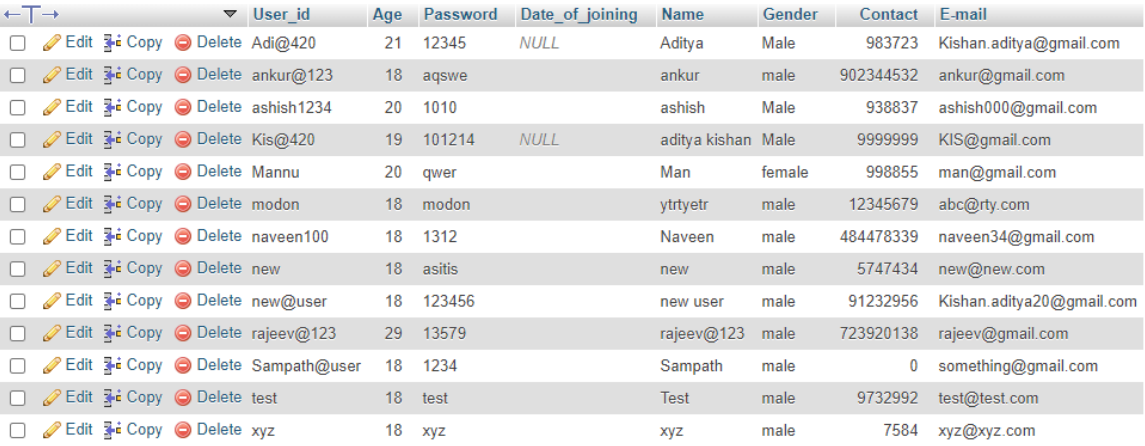
25

Male

99999

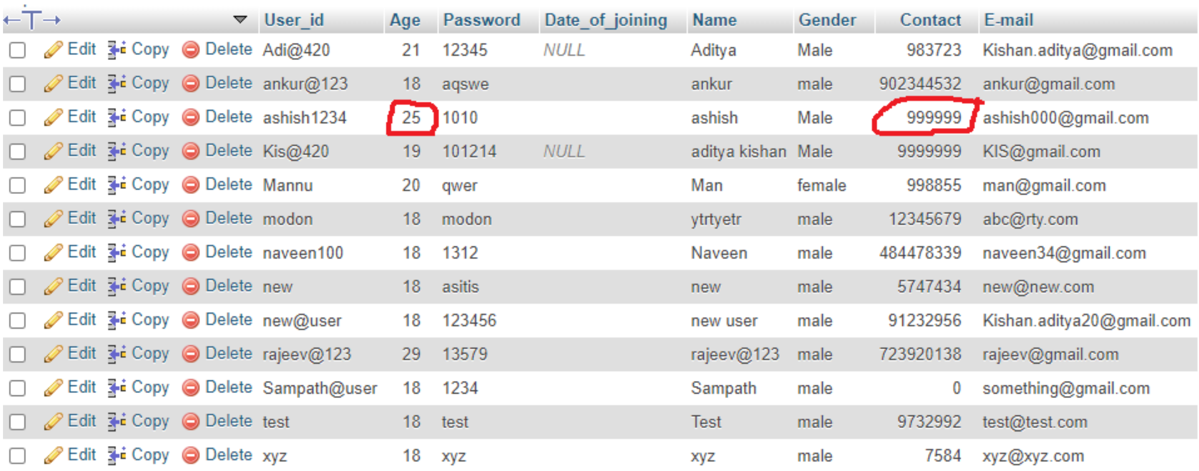
ashish000@gm

Before edit



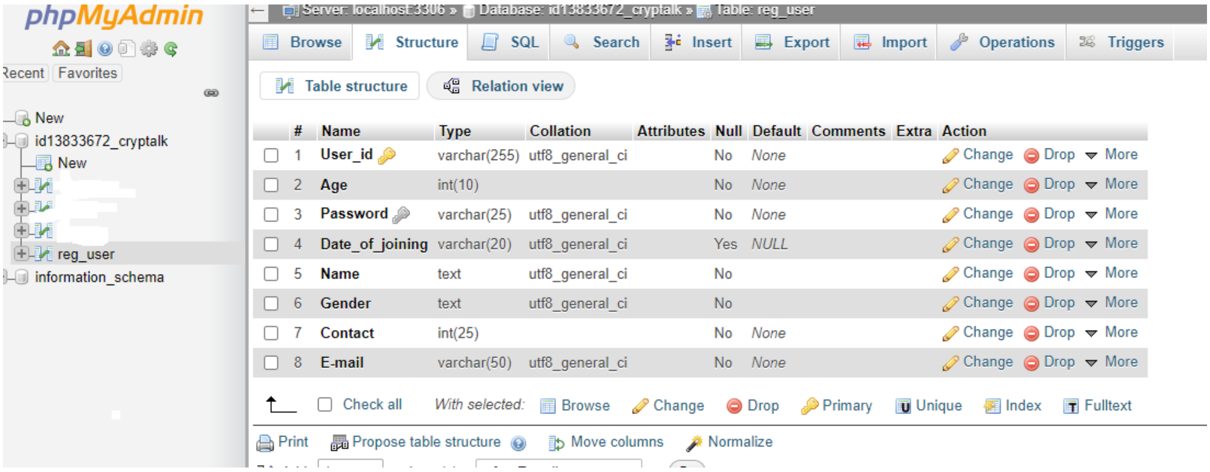
←T→ ▼	User_id	Age	Password	Date_of_joining	Name	Gender	Contact	E-mail
□ Edit Copy Delete	Adi@420	21	12345	NULL	Aditya	Male	983723	Kishan.aditya@gmail.com
□ Edit Copy Delete	ankur@123	18	aqswe		ankur	male	902344532	ankur@gmail.com
□ Edit Copy Delete	ashish1234	20	1010		ashish	Male	938837	ashish000@gmail.com
□ Edit Copy Delete	Kis@420	19	101214	NULL	aditya kishan	Male	9999999	KIS@gmail.com
□ Edit Copy Delete	Mannu	20	qwer		Man	female	998855	man@gmail.com
□ Edit Copy Delete	modon	18	modon		ytrtyetr	male	12345679	abc@rty.com
□ Edit Copy Delete	naveen100	18	1312		Naveen	male	484478339	naveen34@gmail.com
□ Edit Copy Delete	new	18	asitis		new	male	5747434	new@new.com
□ Edit Copy Delete	new@user	18	123456		new user	male	91232956	Kishan.aditya20@gmail.com
□ Edit Copy Delete	rajeev@123	29	13579		rajeev@123	male	723920138	rajeev@gmail.com
□ Edit Copy Delete	Sampath@user	18	1234		Sampath	male	0	something@gmail.com
□ Edit Copy Delete	test	18	test		Test	male	9732992	test@test.com
□ Edit Copy Delete	xyz	18	xyz		xyz	male	7584	xyz@xyz.com

After edit



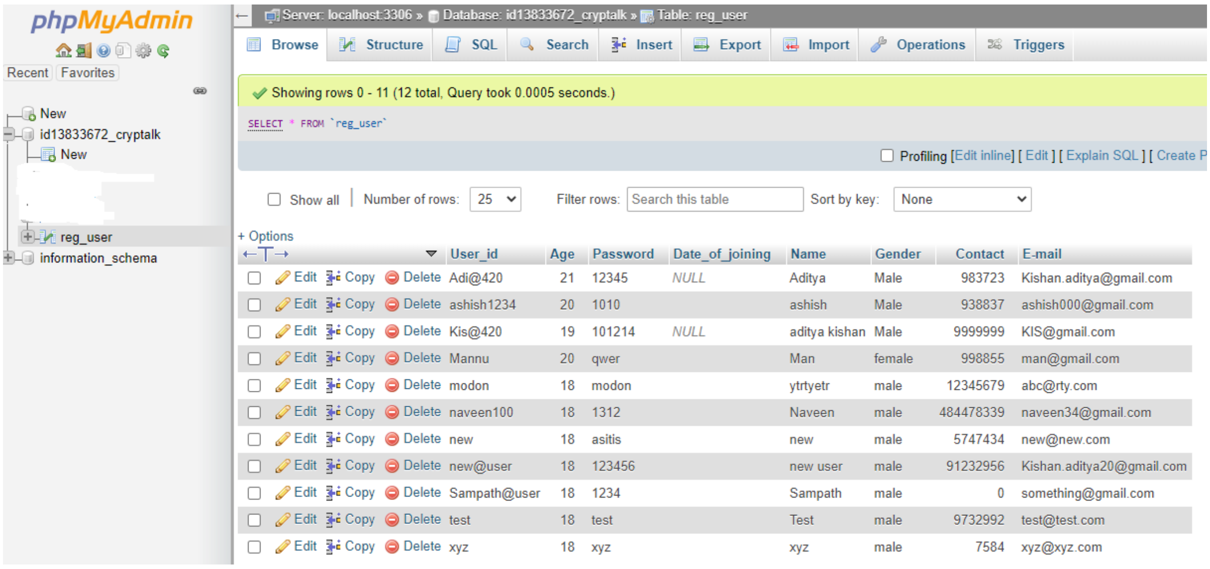
←T→ ▼	User_id	Age	Password	Date_of_joining	Name	Gender	Contact	E-mail
□ Edit Copy Delete	Adi@420	21	12345	NULL	Aditya	Male	983723	Kishan.aditya@gmail.com
□ Edit Copy Delete	ankur@123	18	aqswe		ankur	male	902344532	ankur@gmail.com
□ Edit Copy Delete	ashish1234	25	1010		ashish	Male	999999	ashish000@gmail.com
□ Edit Copy Delete	Kis@420	19	101214	NULL	aditya kishan	Male	9999999	KIS@gmail.com
□ Edit Copy Delete	Mannu	20	qwer		Man	female	998855	man@gmail.com
□ Edit Copy Delete	modon	18	modon		ytrtyetr	male	12345679	abc@rty.com
□ Edit Copy Delete	naveen100	18	1312		Naveen	male	484478339	naveen34@gmail.com
□ Edit Copy Delete	new	18	asitis		new	male	5747434	new@new.com
□ Edit Copy Delete	new@user	18	123456		new user	male	91232956	Kishan.aditya20@gmail.com
□ Edit Copy Delete	rajeev@123	29	13579		rajeev@123	male	723920138	rajeev@gmail.com
□ Edit Copy Delete	Sampath@user	18	1234		Sampath	male	0	something@gmail.com
□ Edit Copy Delete	test	18	test		Test	male	9732992	test@test.com
□ Edit Copy Delete	xyz	18	xyz		xyz	male	7584	xyz@xyz.com

Registered user table structure



	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
□	1	User_id	varchar(255)	utf8_general_ci		No	None			Change Drop More
□	2	Age	int(10)			No	None			Change Drop More
□	3	Password	varchar(25)	utf8_general_ci		No	None			Change Drop More
□	4	Date_of_joining	varchar(20)	utf8_general_ci		Yes	NULL			Change Drop More
□	5	Name	text	utf8_general_ci		No				Change Drop More
□	6	Gender	text	utf8_general_ci		No				Change Drop More
□	7	Contact	int(25)			No	None			Change Drop More
□	8	E-mail	varchar(50)	utf8_general_ci		No	None			Change Drop More

User table



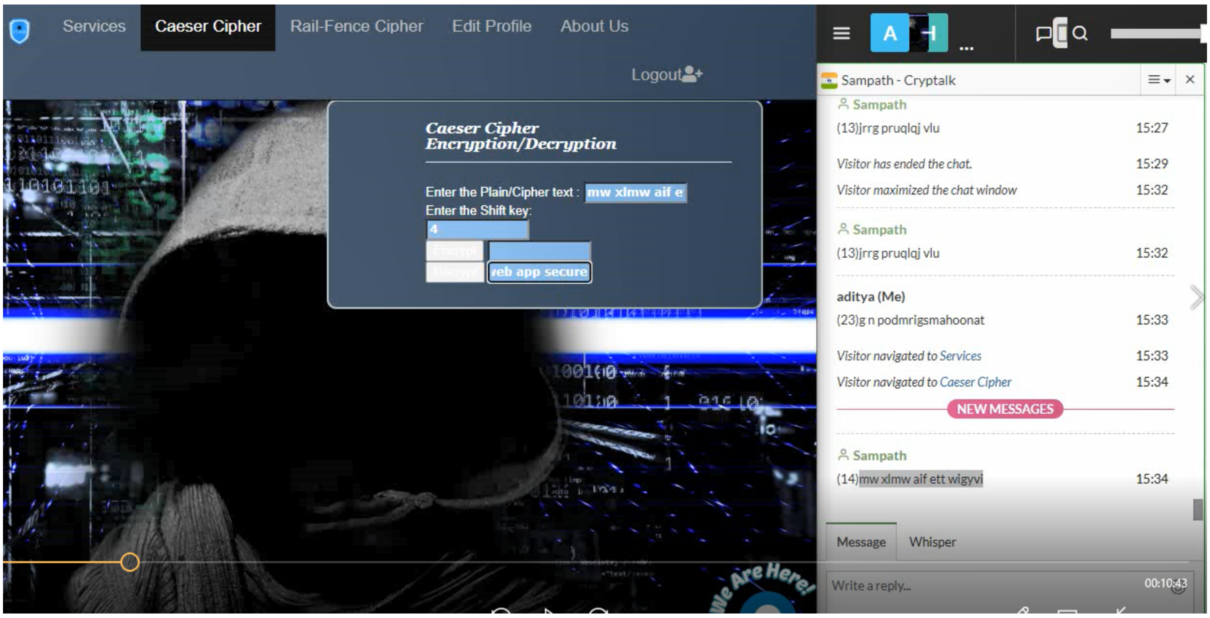
✓ Showing rows 0 - 11 (12 total, Query took 0.0005 seconds.)

```
SELECT * FROM `reg_user`
```

□ Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

		User_id	Age	Password	Date_of_joining	Name	Gender	Contact	E-mail
□	Edit Copy Delete	Adi@420	21	12345	NULL	Aditya	Male	983723	Kishan.aditya@gmail.com
□	Edit Copy Delete	ashish1234	20	1010		ashish	Male	938837	ashish000@gmail.com
□	Edit Copy Delete	Kis@420	19	101214	NULL	aditya kishan	Male	9999999	KIS@gmail.com
□	Edit Copy Delete	Mannu	20	qwer		Man	female	998855	man@gmail.com
□	Edit Copy Delete	modon	18	modon		ytrtyetr	male	12345679	abc@rty.com
□	Edit Copy Delete	naveen100	18	1312		Naveen	male	484478339	naveen34@gmail.com
□	Edit Copy Delete	new	18	asitis		new	male	5747434	new@new.com
□	Edit Copy Delete	new@user	18	123456		new user	male	91232956	Kishan.aditya20@gmail.com
□	Edit Copy Delete	Sampath@user	18	1234		Sampath	male	0	something@gmail.com
□	Edit Copy Delete	test	18	test		Test	male	9732992	test@test.com
□	Edit Copy Delete	xyz	18	xyz		xyz	male	7584	xyz@xyz.com

Chat screenshot



Caeser Cipher Encryption/Decryption

Enter the Plain/Cipher text : mw xlmw aif e

Enter the Shift key: 4

veb app secure

Sampath - Cryptalk

Sampath
(13)jrrg pruqlqj vlu 15:27

Visitor has ended the chat. 15:29

Visitor maximized the chat window 15:32

Sampath
(13)jrrg pruqlqj vlu 15:32

aditya (Me)
(23)g n podmrigsmahoonat 15:33

Visitor navigated to Services 15:33

Visitor navigated to Caeser Cipher 15:34

Sampath
(14)mw xlmw aif ett wigyvi 15:34

Write a reply... 00:10:43

Project demo link: https://drive.google.com/file/d/1S3kzH4skUNlM2ADL39NkffFgegLvtU9O/view?usp=sharing

Ppt link: https://drive.google.com/file/d/1Pw8pDb2wljAHBYcQVq-jhcagK7ofuSpW/view?usp=sharing