SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING

INFORMATION AND SYSTEM SECURITY-SWE3002

Review-3

Team Members

P. Harsha chandan Reddy	-	16MIS0182
P. Aravind Reddy	-	16MIS0371

Guided by: Jeyanthi N

Slot: F1+TF1

Title: Password protection using a new encryption process

Abstract:

A password should be encrypted to protect against attackers who gain read-only access to the database where a server stores whatever it needs to verify passwords. Encrypting a password is typically used to protect it from eavesdropping.

Introduction:

Now a days password encrpyion plays a major role in securing the user details.This password encrption can be done in many ways, every application in real world use password encrytion storage in different ways.One application may use hashing processes and other may use any algorithms on their own according to their satisfactory and complexity.

In this paper we are going to explain a new password or data encryption process .

Process:

Firstly user need to sign up, in this process the password will be encrypted and saved in database. so that middle person who are dealing with database works can not view password. If user already exist he can directly skip signup.

After submitting the registration page it will be redirected to Login page which contains a field where user need to submit UserId.

Based on UserId , here undergoes two processes.

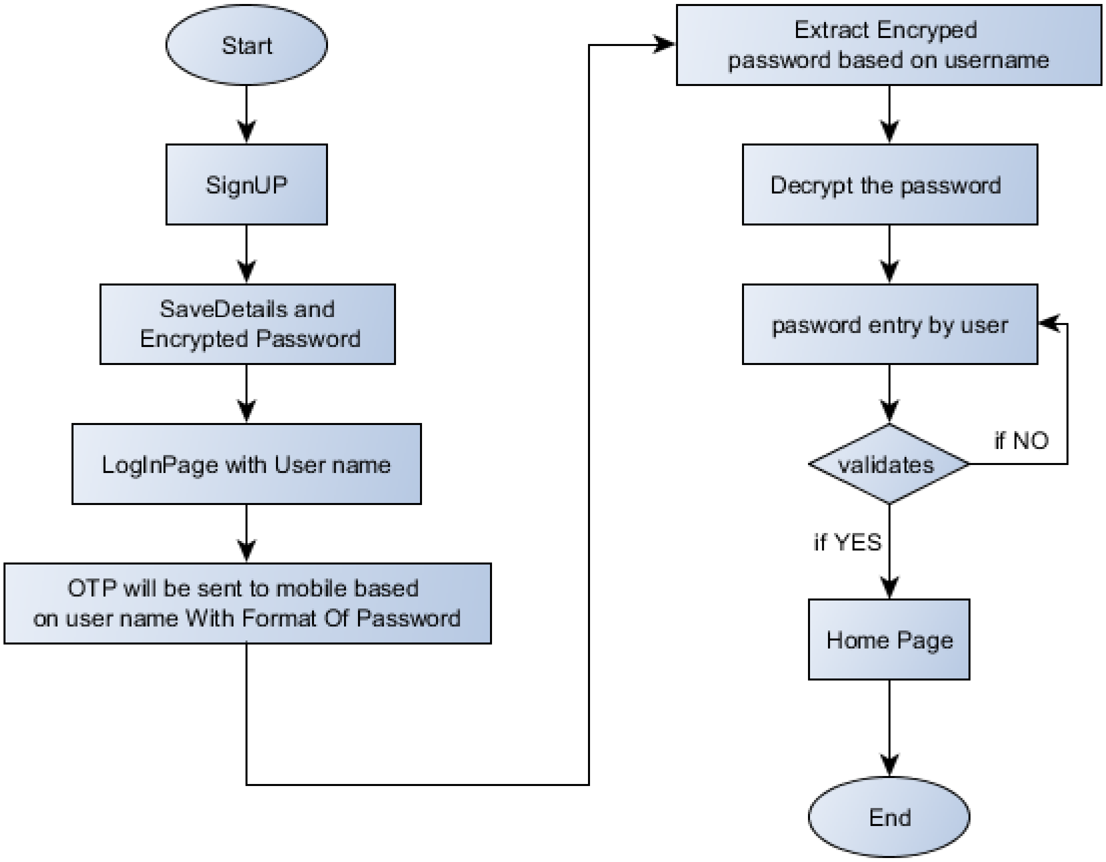
1) Password is fetched from database
2) Phone number is fetched from database

Password that is fetched is decrypted to undergo validation

OTP(Random Generation) will be send to registered phone number including format of password entry which is decided randomly.(eg XXXXOTP or OTPXXXX)

Finally ,Validation is done to authorize the user.

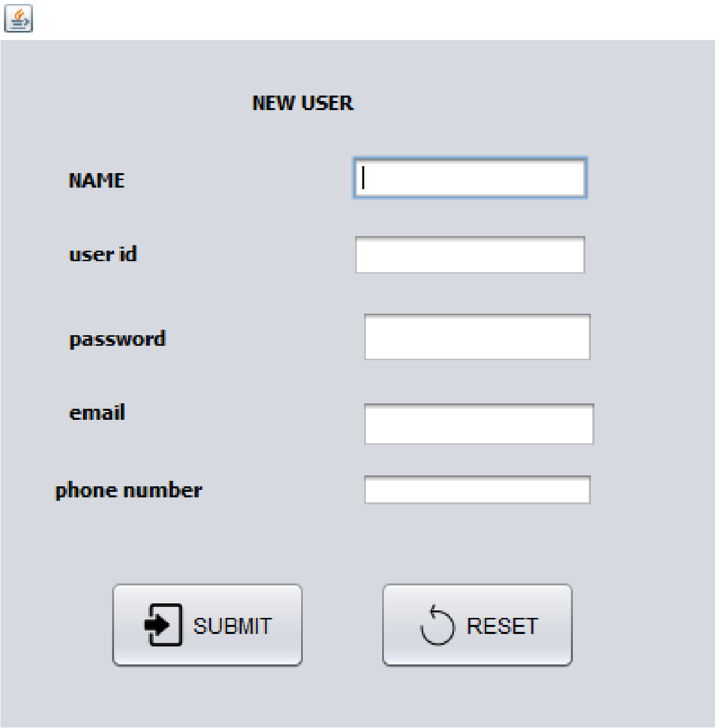
Figure -1 overall flow


Start
SignUP
SaveDetails and Encrypted Password
LogInPage with User name
OTP will be sent to mobile based on user name With Format Of Password
Extract Encryped password based on username
Decrypt the password
pasword entry by user
validates
if NO
if YES
Home Page
End

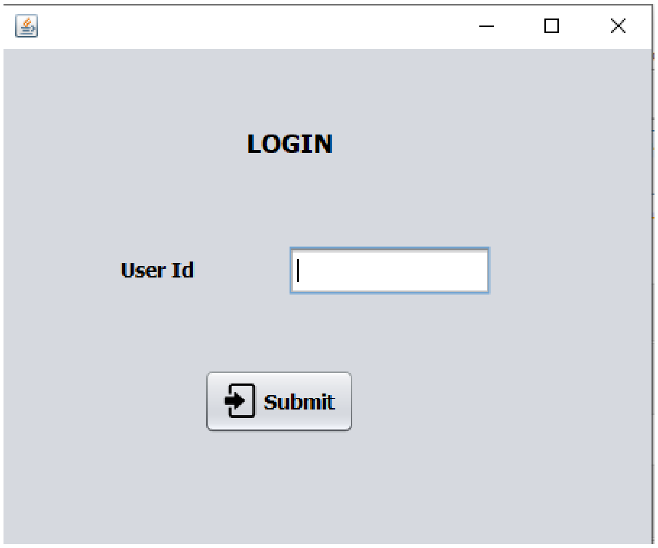
This process is done using

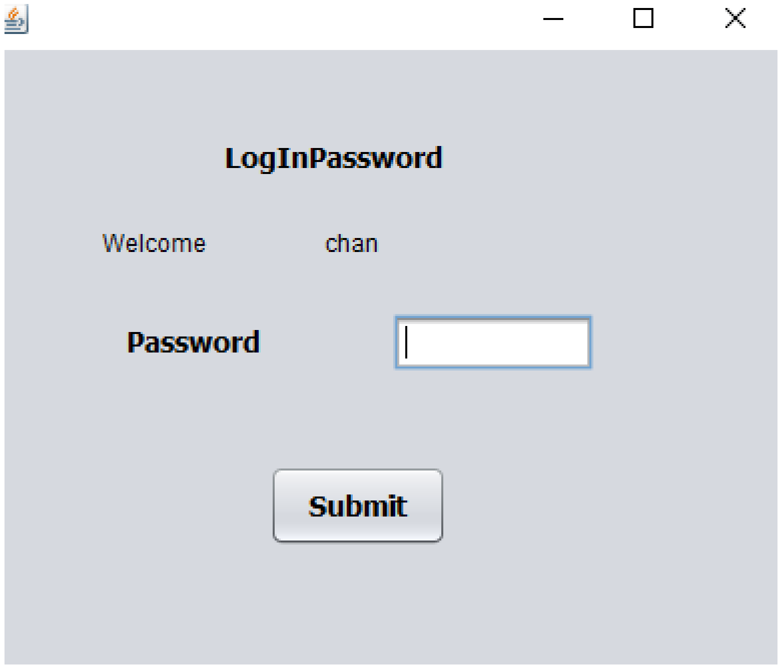
1) Netbeans to create a sample application
2) Wamp server as a Database
3) Text local website to send OTP in message format.

Registration Page:



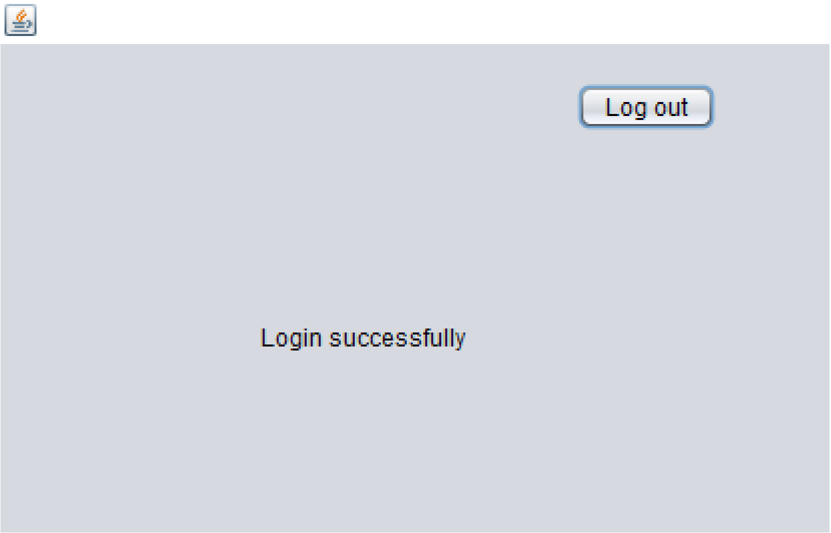
LogIn page:





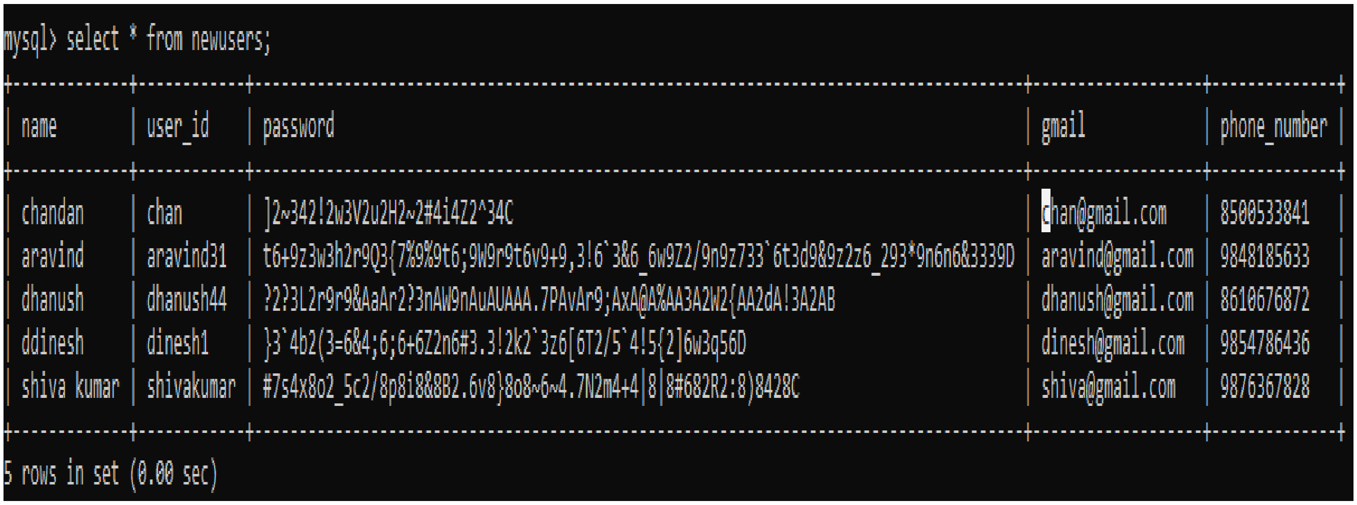
Welcome chan

Homepage



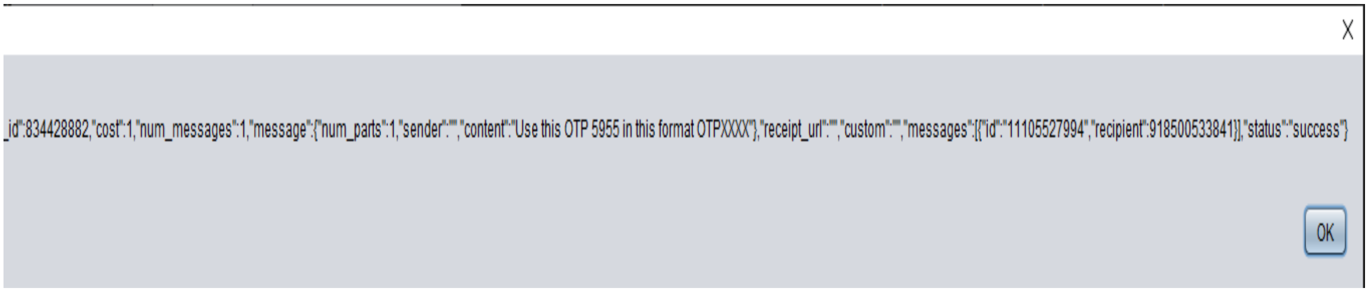
Login successfully

Database Value:



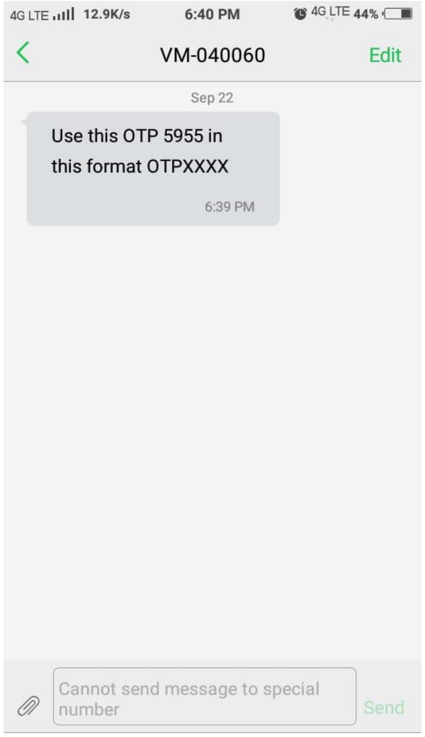
```
mysql> select * from newusers;
+-------------+------------+--------------------------------------------------------------------------------------+-------------------+--------------+
| name        | user_id    | password                                                                             | gmail             | phone_number |
+-------------+------------+--------------------------------------------------------------------------------------+-------------------+--------------+
| chandan     | chan       | ]2~342!2w3V2u2H2~2#4i4Z2^34C                                                         | chan@gmail.com    | 8500533841   |
| aravind     | aravind31  | t6+9z3w3h2r9Q3{7%9%9t6;9W9r9t6v9+9,3!6`3&6_6w9Z2/9n9z733`6t3d9&9z2z6_293*9n6n6&3339D | aravind@gmail.com | 9848185633   |
| dhanush     | dhanush44  | ?2?3L2r9r9&AaAr2?3nAW9nAuAUAAA.7PAvAr9;AxA@A%AA3A2W2{AA2dA!3A2AB                     | dhanush@gmail.com | 8610676872   |
| ddinesh     | dinesh1    | }3`4b2(3=6&4;6;6+6Z2n6#3.3!2k2`3z6[6T2/5`4!5{2]6w3q56D                               | dinesh@gmail.com  | 9854786436   |
| shiva kumar | shivakumar | #7s4x8o2_5c2/8p8i8&8B2.6v8}8o8~6~4.7N2m4+4|8|8#682R2:8)8428C                         | shiva@gmail.com   | 9876367828   |
+-------------+------------+--------------------------------------------------------------------------------------+-------------------+--------------+
5 rows in set (0.00 sec)
```

OTP process:



```
_id":834428882,"cost":1,"num_messages":1,"message":{"num_parts":1,"sender":"","content":"Use this OTP 5955 in this format OTPXXXX"},"receipt_url":"","custom":"","messages":[{"id":"11105527994","recipient":918500533841}],"status":"success"}
```

OTP Received to mobile with format:



Use this OTP 5955 in this format OTPXXXX

Encryption Process:

The password given by the user will be saved in database in encrypted manner.

A huge set of characters will be intialized in an array.

Initially a space value will be generated.

Each two characters of the password will be inserted with randomly generated characters acoording to the sapce value.

Now the total number of characters will serve as a base value or a key.

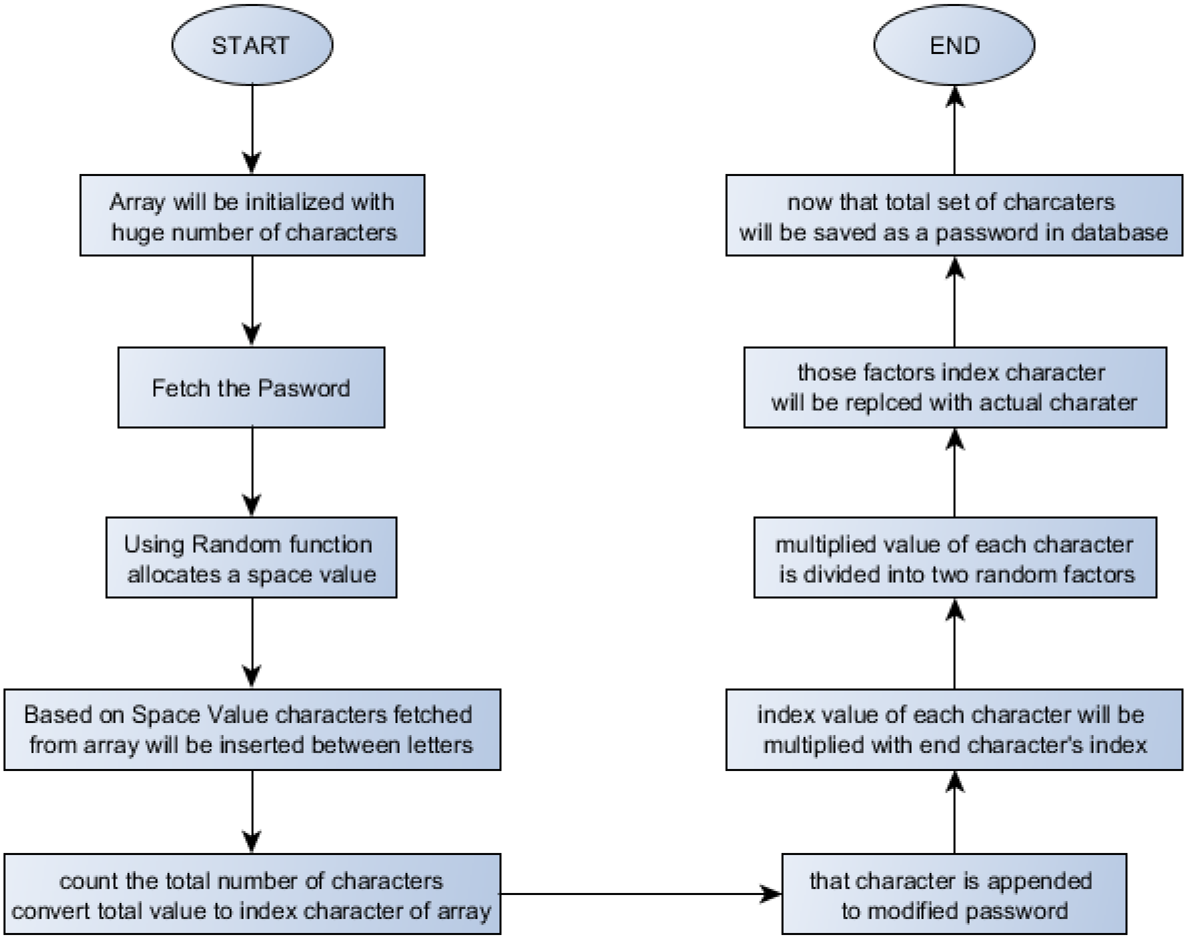
Each character present in the password will be multiplied with base value.

Now the multiplied value will be divided into two factors and the index charcter will be fetched from array using the two factors .

Now the character before multiplication will be replced with those two characters (i.e factors)and this process will be repeated for whole password.

Now the index charcater of the base value will be appended to the modified password and it is saved in the database.

Figure -2 Encryption Process


START
Array will be initialized with huge number of characters
Fetch the Pasword
Using Random function allocates a space value
Based on Space Value characters fetched from array will be inserted between letters
count the total number of characters convert total value to index character of array
that character is appended to modified password
index value of each character will be multiplied with end character's index
multiplied value of each character is divided into two random factors
those factors index character will be replced with actual charater
now that total set of charcaters will be saved as a password in database
END

Decryption Process:

The password that is saved in the database will be fetched

The same array used in encryption is used here.

Array index value of last character present in password will be fetched.

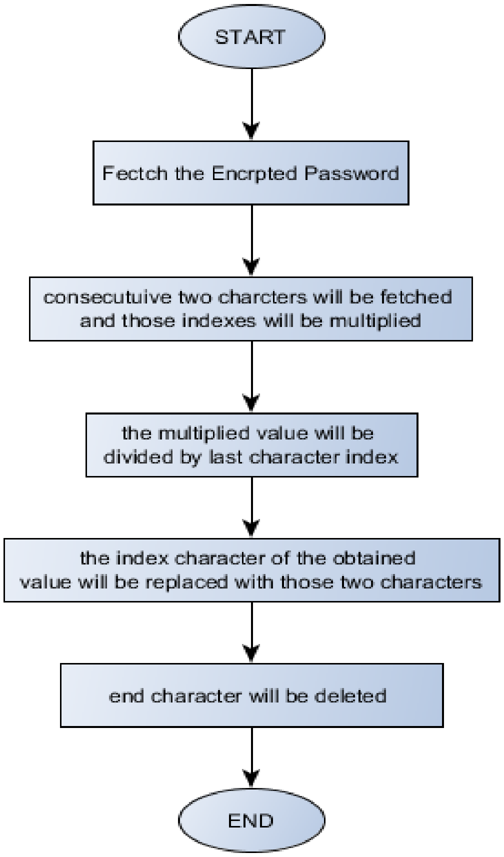
Now two consecutive character of paasword will be multiplied (index values are taken from array)

Now the multiplied value will be divided with the base value

The output value is used to fetch the characater from the array which is replaced with those two characters.

Finally the last character will be deleted from the string(i.e Base value will be deleted)

Figure -3 Decryption Process


START
Fectch the Encrpted Password
consecutuive two charcters will be fetched and those indexes will be multiplied
the multiplied value will be divided by last character index
the index character of the obtained value will be replaced with those two characters
end character will be deleted
END

Encryption code:

```
String aa=jTextField1.getText();

     String bb=jTextField2.getText();

     String c=jPasswordField1.getText();

     String d;

     d = jTextField4.getText();

      String f;

     f = jTextField5.getText();
```

```
       String pass=c,rstring="",as,en="",we;

        String option[]=
{"$","1","2","3","4","5","6","7","8","9","0","A","B",
"C","D","E","F","G","H","I","J","K","L","M","N","O
","P","Q","R","S","T","U","V","W","X","Y","Z","@
","a","b","c","d","e","f","g","h","i","j","k","l","m","n
","o","p","q","r","s","t","u","v","w","x","y","z","#","*
","!","%","^","&","(",")","_","-
","+","=","~","?","/","[","]","{","}","|","`",":",";",",","
.","<"};

        System.out.println((int)option.length);
```

```
int spv=0,a=0,b=0,l=0,qw;
int spacearr[]={2,3,4};
int sp;
int randomNumber;
int pkey=(((int)pass.length())*(spv+1))-spv;
System.out.println(pkey);
Random k=new Random();
randomNumber=k.nextInt(option.length);
sp=k.nextInt(spacearr.length);
spv=spacearr[sp];
System.out.println(spv);
System.out.println(option[randomNumber]);


for(int i=0;i<(int)pass.length()-1;i++)
{
    as="";
    for(int j=0;j<spv;j++)
    {
        Random r=new Random();
        randomNumber=r.nextInt(option.length);
        as=as+option[randomNumber];
    }
    rstring=rstring+pass.charAt(i)+as;
}
rstring=rstring+pass.charAt((int)pass.length()-1);
System.out.println(rstring);
String df;
for(int q=0;q<=(int)rstring.length()-1;q++)
{
```

```
 qw=-1;
l=0;

for(int o=0;;o++)
{
    qw++;
    df=option[qw];
    if(rstring.charAt(q)==df.charAt(0))
    {
        break;
    }
}

 l=qw*pkey;

 if(l==1 || l==2 || l==3 || l==5 || l==7 || l==11 || l==15 || l==17 || l==19)
 {
     for(int i=1;i<=l;i++)
     {
         for(int j=1;j<=l;j++)
         {
             if(l==(i*j))
             {
                 a=i;
                 b=j;
                 break;
             }
         }
     }
 }
 else
```

```
  {

      for(int i=2;i<=l;i++)
      {
        for(int j=2;j<=l;j++)
        {
          if(l==(i*j))
          {
            if(i<90 && j<90)
        {

            a=i;
            b=j;
            break;
        }
          }
        }
      }

  }
  System.out.println(l+"="+a+"*"+b);
  en=en+option[a]+option[b];
}
en=en+option[pkey]+option[10+spv];
System.out.println(en);
```

Decryption code:

```
Statement statement = conn.createStatement();
ResultSet result = statement.executeQuery(sql);
int count = 0;
while (result.next()){
  String user = result.getString("user_id");
  String pass = result.getString("password");

      String en=pass,dec="";
    String decry;
    String dec2,dec4;
    String aa,mainstr;
    mainstr="";
    String main;
    main="";
    int cou;
    int cou2;
    int ssaa=0;
    int ssssaa;
    String ssss;
    ssss="";
    cou2=0;
    String ss;
    ss="";
    ss=ss+en.charAt((int)(en.length()-1));
    dec2="";
    dec4="";
    int n;
    int aaaa[];
    int ssssaaaa[];
    n=0;
    String option[]=
{"$","1","2","3","4","5","6","7","8","9","0","A","B",
"C","D","E","F","G","H","I","J","K","L","M","N","O
","P","Q","R","S","T","U","V","W","X","Y","Z","@
","a","b","c","d","e","f","g","h","i","j","k","l","m","n
","o","p","q","r","s","t","u","v","w","x","y","z","#","*
","!","%","^","&","(",")","_","-
","+","=","~","?","/","[","]","{","}","|","`",":",";",","
.","<"};
    int numb=(int)en.length();
    String sp="";sp=sp+en.charAt(numb-1);
    int spv=0;
    for(int ke=0;;ke++)
    {
     ssss="";
     ssss=ssss+option[ke];
        if((sp.charAt(0))==ssss.charAt(0))
        {
            break;
        }
        spv++;
    }
    spv=spv-10;
    System.out.println(spv);
```

```
    for(int i=0;i<(int)en.length()-2;i++)
    {
      dec=dec+en.charAt(i);
    }
    System.out.println(dec);
    dec2=dec;
    int inc;
    inc=0;
    if(spv==2)
    {
    for(int i=0;i<25;i++)
    {
     if((int)dec.length()==8+(i*(6)))
     {
       n=2+i;
       break;
     }
    }
  }

    if(spv==3)
    {
    for(int i=0;i<25;i++)
    {
     if((int)dec.length()==10+(i*(8)))
     {
       n=2+i;
       break;
     }
    }
  }
  if(spv==4)
```

```
       {
       for(int i=0;i<25;i++)
       {
        if((int)dec.length()==12+(i*(10)))
        {
            n=2+i;
            break;
        }
       }
    }
System.out.println(n);
       for(int i=0;i<n;i++)
       {
       for(int j=inc;j<inc+2;j++)
       {
           dec4=dec4+dec.charAt(j);
       }
       inc=inc+((spv*2)+2);
    }
       System.out.println(dec4);
       System.out.println(ss.charAt(0));
       aaaa=new int[(int)dec4.length()];
       ssssaaaa=new int[((int)dec4.length())/2];
       for(int i=0;i<(int)dec4.length();i++)
       {
        cou=0;
        aa="";
           aa=aa+dec4.charAt(i);
           for(int j=0;;j++)
           {
               ssss="";
               ssss=ssss+option[j];
```

```
               if(aa.charAt(0)==ssss.charAt(0))
               {
                   break;
               }
               cou++;
           }
          aaaa[i]=cou;
          //System.out.println(cou);
         }
         for(int k=0;;k++)
          {
               ssss="";
               ssss=ssss+option[k];
               if(en.charAt((int)en.length()-
2)==ssss.charAt(0))
               {
                   break;
               }
               cou2++;
          }
          System.out.println(cou2);
         //System.out.println(option[38]);
          for(int i=0;i<(int)dec4.length();i=i+2)
          {
               mainstr="";
               for(int j=i+1;j<=i+1;j++)
               {
                   ssaa=aaaa[i]*aaaa[j];
               }


               mainstr=mainstr+option[ssaa/cou2];
```

```
             main=main+mainstr.charAt(0);
           }
          System.out.println(main);
          System.out.println(ran1);
          System.out.println(ran2);

    System.out.format("%s, %s\n",user,pass);

    if(ran1.equals("XXXXOTP"))
    {
        main=main+ran2;
        System.out.println(main);
        if(main.equals(jPasswordField1.getText()))
     {
         new homepage().setVisible(true);
     }
     else
     {
         System.out.println("error in username or
password");
     }
    }
    if(ran1.equals("OTPXXXX"))
    {

        main=ran2+main;
        System.out.println(main);
        if(main.equals(jPasswordField1.getText()))
     {
         new homepage().setVisible(true);
     }
     else
```

```
     {
         System.out.println("error in username or
password");
     }
    }
    this.dispose();

}

    if (conn != null) {
        System.out.println("Connected");
    }
    } catch (SQLException ex) {
    ex.printStackTrace();
    }    // TODO add your handling code here:
    }

    /**
     * @param args the command line arguments
     */
    public static void main(String args[]) {
        /* Set the Nimbus look and feel */
        //<editor-fold defaultstate="collapsed" desc="
Look and feel setting code (optional) ">
        /* If Nimbus (introduced in Java SE 6) is not
available, stay with the default look and feel.
         * For details see
http://download.oracle.com/javase/tutorial/uiswing/lo
okandfeel/plaf.html
         */
        try {
            for (javax.swing.UIManager.LookAndFeelInfo info : javax.swing.UIManager.getInstalledLookAndFeels()) {
                if ("Nimbus".equals(info.getName())) {
                    javax.swing.UIManager.setLookAndFeel(info.getClassName());
                    break;
                }
            }
        } catch (ClassNotFoundException ex) {
            java.util.logging.Logger.getLogger(signup.class.getName()).log(java.util.logging.Level.SEVERE, null, ex);
        } catch (InstantiationException ex) {
            java.util.logging.Logger.getLogger(signup.class.getName()).log(java.util.logging.Level.SEVERE, null, ex);
        } catch (IllegalAccessException ex) {
            java.util.logging.Logger.getLogger(signup.class.getName()).log(java.util.logging.Level.SEVERE, null, ex);
        } catch (javax.swing.UnsupportedLookAndFeelException ex) {
            java.util.logging.Logger.getLogger(signup.class.getName()).log(java.util.logging.Level.SEVERE, null, ex);
        }
        //</editor-fold>

        /* Create and display the form */
        java.awt.EventQueue.invokeLater(new Runnable() {
            public void run() {
                new homepage().setVisible(true);
            }
        });
    }
```