package Algorithms;

import java.math.BigInteger;

import java.nio.charset.StandardCharsets;

import java.security.MessageDigest;

import java.security.NoSuchAlgorithmException;

// Java program to calculate SHA hash value

public class HashFunction {

public static byte[] getSHA(String input) throws NoSuchAlgorithmException

{ // Static getInstance method is called with hashing SHA

MessageDigest md = MessageDigest.getInstance("SHA-256"); // digest() method called

// to calculate message digest of an input

// and return array of byte

return md.digest(input.getBytes(StandardCharsets.UTF\_8));

} public static String toHexString(byte[] hash)

{ // Convert byte array into signum representation

BigInteger number = new BigInteger(1, hash);

// Convert message digest into hex value

StringBuilder hexString = new StringBuilder(number.toString(16));

// Pad with leading zeros

while (hexString.length() < 32)

{ hexString.insert(0, '0');} return hexString.toString(); } }

package Algorithms;

import java.io.UnsupportedEncodingException;

import java.security.MessageDigest;

import java.security.NoSuchAlgorithmException;

import java.util.Arrays;

import java.util.Base64;

import javax.crypto.Cipher;

import javax.crypto.spec.SecretKeySpec;

public class AES {

private static SecretKeySpec secretKey;

private static byte[] key;

public static void setKey(String myKey)

{ MessageDigest sha = null;

try {

key = myKey.getBytes("UTF-8");

sha = MessageDigest.getInstance("SHA-1");

key = sha.digest(key);

key = Arrays.copyOf(key, 16);

secretKey = new SecretKeySpec(key, "AES");

}

catch (NoSuchAlgorithmException e) {

e.printStackTrace();

}

catch (UnsupportedEncodingException e) {

e.printStackTrace();

}

} public static String encrypt(String strToEncrypt, String secret)

{

try

{

setKey(secret);

Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");

cipher.init(Cipher.ENCRYPT\_MODE, secretKey);

return Base64.getEncoder().encodeToString(cipher.doFinal(strToEncrypt.getBytes("UTF-8")));

}

catch (Exception e)

{

System.out.println("Error while encrypting: " + e.toString());

}

return null;

}public static String decrypt(String strToDecrypt, String secret { try {

setKey(secret);

Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5PADDING");

cipher.init(Cipher.DECRYPT\_MODE, secretKey);

return new String(cipher.doFinal(Base64.getDecoder().decode(strToDecrypt)));

}

catch (Exception e)

{ System.out.println("Error while decrypting: " + e.toString());

}

return null;

}

/\*public static void main(String[] args)

{ final String secretKey = "MYKEY234@E1";

String originalString = "WELCOME TO INDRA COLLEGE";

String encryptedString = AES.encrypt(originalString, secretKey) ;

String decryptedString = AES.decrypt(encryptedString, secretKey) ;

System.out.println(originalString);

System.out.println(encryptedString);

System.out.println(decryptedString);

}\*/

}<!DOCTYPE HTML>

<html>

<%@page import="Algorithms.\*"%>

<head>

<title>Authentication by Encrypted Negative Password</title>

<meta name="description" content="website description" />

<meta name="keywords" content="website keywords, website keywords" />

<meta http-equiv="content-type" content="text/html; charset=UTF-8" />

<link rel="shortcut icon" type="image/x-icon" href="images/brainstorming\_alternative.png"/>

<link rel="stylesheet" type="text/css" href="css/style.css" />

<!-- modernizr enables HTML5 elements and feature detects -->

<script type="text/javascript" src="js/modernizr-1.5.min.js"></script> <script>

function validation(){

var uname=document.ureg.username.value;

var pass=document.ureg.password.value;

var cpass=document.ureg.cpassword.value;

var mail=document.ureg.mail.value;

var name=document.ureg.name.value;

var ph=document.ureg.mobile.value;

if(name==0){

alert("Enter name");

document.ureg.name.focus();

return false;

}

if(uname==0){

alert("Enter username");

document.ureg.username.focus();

return false;

}

if(pass==0){

alert("Enter password");

document.ureg.password.focus();

return false;

}

if(cpass!=pass){

alert("Incorrect password");

document.ureg.cpassword.focus();

return false;

} if(mail==0){

alert("Enter mailid");

document.ureg.mail.focus();

return false;

}

if(ph==0){

alert("Enter your mobile no");

document.ureg.mobile.focus();

return false;

}

if(isNaN(ph)){

alert("Invalid phoneno");

document.ureg.mobile.focus();

return false;

}

}

</script>

<style>

input{

width: 200px;

height: 25px;

background-color: #D5D5D5;

}

#but{

width: 75px;

height: 25px;

}

</style>

</head>

<body>

<%

if(request.getParameter("error")!=null){

out.println("<script>alert('The username already exists!')</script>");

}

%>

<div id="main">

<header>

<div id="logo">

<div id="logo\_text">

<!-- class="logo\_colour", allows you to change the colour of the text -->

<pre><h1><img src="images/cooltext345289362861870.png" width="900" height="100"></h1>

</div>

</div>

<nav>

<ul class="sf-menu" id="nav">

<li class="selected"><a href="index.html">Home</a></li>

<li><a href="admin.jsp">Admin</a></li>

<li><a href="#">User</a>

<ul>

<li><a href="user.jsp">Login</a></li>

<li><a href="register.jsp">Register</a></li>

</ul>

</li> </ul>

</nav>

</header>

<div id="site\_content">

<div id="sidebar\_container">

<div class="gallery">

<ul class="images">

<li class="show"><img width="450" height="450" src="images/rphase.PNG" alt="photo\_one" /></li>

<li><img width="450" height="450" src="images/c2.jpg" alt="photo\_two" /></li>

<li><img width="450" height="450" src="images/c3.jpg" alt="photo\_three" /></li>

<li><img width="450" height="450" src="images/c4.jpg" alt="photo\_four" /></li>

<li><img width="450" height="450" src="images/c5.jpg" alt="photo\_five" /></li>

</ul> </div> </div>

<div id="content">

<fieldset style="background-color: #70D4E6;">

<center>

<h2 class="title"style="color: red;font-size: 20px;">Encrypted Negative Password Function</h2>

</center>

<form action="doRegistration1.jsp" name="ureg" style="position: relative;left: 110px;" method="post" onsubmit="return validation()">

<!-- USERNAME:<br>-->

<%String uname=(String)session.getAttribute("uname");

String pwd=(String)session.getAttribute("pwd");

String hash=request.getParameter("hpassword");

String npwd=request.getParameter("npassword");

%>

<B><font color="brown">User Name:<BR>

<input type="text" name="username" value="<%=uname%>" readonly><br></br>

<!-- PASSWORD:<br>-->

Plain Password:<BR>

<input type="password" name="password" value="<%=pwd%>" readonly><br></br>

Hash Password:<BR>

<textarea name="hpassword" rows="5" cols="40" readonly><%=hash%></textarea><br></br>

Negative Password:<BR>

<textarea name="npassword" rows="5" cols="40" readonly><%=npwd%></textarea><br></br>

Encrypted Negative Password (ENP):<BR>

<%

String encrypted\_data=new AES().encrypt(npwd,hash);

%>

<textarea name="epassword" rows="5" cols="40" readonly><%=encrypted\_data%></textarea><br></br>

&nbsp;<input type="submit" id="but" value="Registration" style="background-color: yellowgreen;color: #ffffff;width:200px"/>

&nbsp;&nbsp; <br></br></form>

</fieldset>

</div></div><footer>

<p>Copyright &copy; Jpinfotech. All Rights Reserved.</p>

</footer>

</div>

<p>&nbsp;</p>

<!-- javascript at the bottom for fast page loading -->

<script type="text/javascript" src="js/jquery.js"></script>

<script type="text/javascript" src="js/jquery.easing-sooper.js"></script>

<script type="text/javascript" src="js/jquery.sooperfish.js"></script>

<script type="text/javascript" src="js/image\_fade.js"></script>

<script type="text/javascript">

$(document).ready(function() {

$('ul.sf-menu').sooperfish();

});

</script>

</body>

</html>

<!DOCTYPE HTML>

<html>

<%@page import="Algorithms.\*"%>

<head>

<title>Authentication by Encrypted Negative Password</title>

<meta name="description" content="website description" />

<meta name="keywords" content="website keywords, website keywords" />

<meta http-equiv="content-type" content="text/html; charset=UTF-8" />

<link rel="shortcut icon" type="image/x-icon" href="images/brainstorming\_alternative.png"/>

<link rel="stylesheet" type="text/css" href="css/style.css" />

<!-- modernizr enables HTML5 elements and feature detects -->

<script type="text/javascript" src="js/modernizr-1.5.min.js"></script>

<script>

function validation(){

var uname=document.ureg.username.value;

var pass=document.ureg.password.value;

var cpass=document.ureg.cpassword.value;

var mail=document.ureg.mail.value;

var name=document.ureg.name.value;

var ph=document.ureg.mobile.value;

if(name==0){

alert("Enter name");

document.ureg.name.focus();

return false;

}

if(uname==0){

alert("Enter username");

document.ureg.username.focus();

return false;}

if(pass==0){

alert("Enter password");

document.ureg.password.focus();

return false;

}

if(cpass!=pass){

alert("Incorrect password");

document.ureg.cpassword.focus();

return false;

}if(mail==0){

alert("Enter mailid");

document.ureg.mail.focus();

return false;

}

if(ph==0){

alert("Enter your mobile no");

document.ureg.mobile.focus(); return false;

}

if(isNaN(ph)){

alert("Invalid phoneno");

document.ureg.mobile.focus();

return false;

}

}

</script>

<style>

input{

width: 200px;

height: 25px;

background-color: #D5D5D5;

}

#but{

width: 75px;

height: 25px;

}

</style>

</head>

<body>

<%

if(request.getParameter("error")!=null){

out.println("<script>alert('The username already exists!')</script>");

} %>

<div id="main">

<header>

<div id="logo">

<div id="logo\_text">

<!-- class="logo\_colour", allows you to change the colour of the text -->

<pre><h1><img src="images/cooltext345289362861870.png" width="900" height="100"></h1> </div>

</div>

<nav>

<ul class="sf-menu" id="nav">

<li class="selected"><a href="index.html">Home</a></li>

<li><a href="admin.jsp">Admin</a></li>

<li><a href="#">User</a>

<ul>

<li><a href="user.jsp">Login</a></li>

<li><a href="register.jsp">Register</a></li>

</ul>

</li> </ul>

</nav>

</header>

<div id="site\_content">

<div id="sidebar\_container">

<div class="gallery">

<ul class="images">

<li class="show"><img width="450" height="450" src="images/rphase.PNG" alt="photo\_one" /></li>

<li><img width="450" height="450" src="images/c2.jpg" alt="photo\_two" /></li>

<li><img width="450" height="450" src="images/c3.jpg" alt="photo\_three" /></li>

<li><img width="450" height="450" src="images/c4.jpg" alt="photo\_four" /></li>

<li><img width="450" height="450" src="images/c5.jpg" alt="photo\_five" /></li>

</ul>

</div>

</div>

<div id="content">

<fieldset style="background-color: #70D4E6;">

<center>

<h2 class="title"style="color: red;font-size: 20px;">Negative Password Function</h2>

</center>

<form action="ENP\_Encryption\_Process.jsp" name="ureg" style="position: relative;left: 110px;" method="post" onsubmit="return validation()">

<!-- USERNAME:<br>-->

<%String uname=(String)session.getAttribute("uname");

String pwd=(String)session.getAttribute("pwd");

String hash=(String)session.getAttribute("hashcode");

%>

<B><font color="brown">User Name:<BR>

<input type="text" name="username" value="<%=uname%>" readonly><br></br>

<!-- PASSWORD:<br>-->

Plain Password:<BR>

<input type="password" name="password" value="<%=pwd%>" readonly><br></br>

Hash Password:<BR>

<textarea name="hpassword" rows="5" cols="30" readonly><%=hash%></textarea><br></br>

<%

String str =hash;

String result = "";String npwd= "";

char[] messChar = str.toCharArray();

for (int i = 0; i < messChar.length; i++) {

result += Integer.toBinaryString(messChar[i]) + " ";

npwd=result.replace("01", "\*");

npwd=result.replace("10", "\*”); }

%>

Generated Negative Password:<BR>

<textarea name="npassword" rows="10" cols="30" readonly><%=npwd%></textarea><br></br>

&nbsp;<input type="submit" id="but" value="Encryption Process" style="background-color: yellowgreen;color: #ffffff;width:200px"/>

&nbsp;&nbsp; <br></br></form>

</fieldset>

</div>

</div>

<footer>

<p>Copyright &copy; Jpinfotech. All Rights Reserved.</p>

</footer>

</div>

<p>&nbsp;</p>

<!-- javascript at the bottom for fast page loading -->

<script type="text/javascript" src="js/jquery.js"></script>

<script type="text/javascript" src="js/jquery.easing-sooper.js"></script>

<script type="text/javascript" src="js/jquery.sooperfish.js"></script>

<script type="text/javascript" src="js/image\_fade.js"></script>

<script type="text/javascript">

$(document).ready(function() {

$('ul.sf-menu').sooperfish();

});

</script>

</body>

</html>