

Practical Lab 7

Student ID: _____

Student Name: _____

Q1. Test the following codes to **encrypt/decrypt** a message using **javascript des functions**.

Test demo1 here: [Demo 1](#)

1. Download **des.js** and put it under your student folder. Set permission as 755.
2. Enter a message, see **the first highlight part**
3. Enter a DES encryption key, see **the second highlight part**
4. Enter a DES decryption key, see **the third highlight part**
5. Link **des.js** to **test_des.html**, see **the fourth highlight part**
6. Call **des encryption functions** to **encrypt** the message using the encryption key, see the **fifth highlight part**
7. Call **des decryption functions** to **decrypt** the ciphertext using the decryption key, see the **sixth highlight part**

test_des.html code as below:

```
<html>
  <body>
    <h1>Lab 7 Demo 1: JavaScript DES test</h1>

    Enter a Message: <input id="message" type="text">
    <br><br>
    Enter a DES encryption key: <input id="DES_Encryption_Key" type="text">
    <br><br>
    <button type="button" onclick="DES_encryption()">Encrypt the Message</button>

    <h3>Encrypted value</h3>
    <p id="encrypted"></p>
    <br><br>
    Enter a DES decryption key to decrypt: <input id="DES_Decryption_Key" type="text">
    <br><br>
    <button type="button" onclick="DES_decryption()">Decrypt the "Encrypted value"</button>
    <h3>Decrypted value</h3>
    <p id="decrypted"></p>

    <script type="text/javascript" src="des.js"></script>
    <script type="text/javascript">
      function DES_encryption() {

        var message = document.getElementById("message").value;

        var key = document.getElementById("DES_Encryption_Key").value;

        // javascript des encryption api
        var encrypted = javascript_des_encryption(key, message);

        document.getElementById("encrypted").innerHTML = encrypted;

      }
      function DES_decryption() {
        var message = document.getElementById("encrypted").innerHTML;

        var key = document.getElementById("DES_Decryption_Key").value;

        // javascript des decryption api
        var decrypted = javascript_des_decryption(key,message);

        document.getElementById("decrypted").innerHTML = decrypted;

      }
    </script>
  </body>
</html>
```

Think: 1. Enter different keys to see the results, what if the encryption key is different from the decryption key?

Q2. Test the following codes to **encrypt/decrypt** a message using **php des functions**.

test Demo2 here: [Demo 2](#)

1. Download **des.php** file and put it under your student folder. Set permission as 755.
2. Include **des.php** to the **test_des.php**, see **first highlight part**
3. Enter a DES key for decryption and encryption, **the second highlight part**
4. Enter a message, see **the third highlight part**
5. Call PHP des encryption API to encrypt the message using the encryption key, see **the fourth highlight part**
6. Call PHP des decryption API to decrypt the ciphertext using the decryption key, see **the fifth highlight part**

test_des.php code as below:

```
<?php
// refer to the des.php file, similar with link to the des.js file (the fourth highlight part in test_des.html)
include('des.php');
?>

<html>
    <body>

        <h1>Lab 7 Demo 2: PHP DES test</h1>

        <?php
            //set up a des key for encryption and decryption
            $key = "this is your key, could be anything";

            //enter a message
            $message = "this is the message";

            echo "key: " . $key . "<br/>";
            echo "message: " . $message . "<br/>";

            // PHP des encryption API (in des.php)
            $ciphertext = php_des_encryption($key, $message);

            echo "DES encrypted message: " . $ciphertext;
            echo "<br/>";

            // PHP des decryption API (in des.php)
            $recovered_message = php_des_decryption($key, $ciphertext);
            echo "DES decrypted message: " . $recovered_message;

        ?>

    </body>

</html>
```

Q3. Based on **Q1**, **Q2**, write a **client.html** and **server.php** to achieve the following:

Preliminaries: DES is a symmetric encryption algorithm, which means the encryption key and the decryption key must be the same, otherwise, the ciphertext cannot be decrypted. Thus, you have to set up a decryption key on the server-side in **server.php** firstly (refer to **the second highlight part** in **test_des.php** of **Q2**), and then run **client.html**, to enter any message and the correct encryption key (Note: it must be the same as the decryption key set in **server.php**), otherwise, the ciphertext cannot be decrypted correctly.

Create the folders/files as below:

Name	Ext	Size	Changed	Rights
..			6/09/2017 10:42:11 AM	rwxr-xr-x
client			6/09/2017 11:02:45 AM	rwxr-xr-x
database			6/09/2017 11:03:50 AM	rwxr-xr-x
server			6/09/2017 10:25:04 AM	rwxr-xr-x

in the folder **server**:

Name	Ext	Size	Changed	Rights
..			6/09/2017 11:03:50 AM	rw-----
des.php		18,3...	5/09/2017 4:58:08 PM	rwxr-xr-x
server.php		897	6/09/2017 10:34:26 AM	rwxr-xr-x

in the folder **database**:

Name	Ext	Size	Changed	Rights
..			6/09/2017 11:03:50 AM	rw-----
database.txt		0	6/09/2017 11:03:59 AM	rw-rw-rw-

in the folder **client**:

Name	Ext	Size	Changed	Rights
..			6/09/2017 11:03:50 AM	rw-----
client.html		882	6/09/2017 10:36:36 AM	rwxr-xr-x
des.js		16,7...	5/09/2017 5:01:07 PM	rwxr-xr-x

Please download **des.js** and **des.php** from **blackboard**, and do not modify them.

Expected outcome: users' input will be encrypted before submitting to server, and will be decrypted on the server side, and store in the database.

Client-side:

1. Enter a message and a DES encryption key
2. Encrypt the message using javascript des encryption API (des.js)
3. Submit the ciphertext

Server-side:

1. Retrieve the ciphertext from client-side
 2. Decrypt the ciphertext using php des decryption API (des.php)
 3. Save the decrypted value to database.
-

For example:

client-side

Lab 7 Answer

Enter the message:

Enter the encryption key:

server-side

Received encrypted Message: 0x84e8f6a9b3ddab795af6f81ed0ac6224

Pre-set decryption key: this is the key

Recovered plaintext message: this is a test

The recovered message has been added to the ../database/database.txt
Go [back](#) to check the database/database.txt

database

```
1 this is a test
```

```
2
```

Answer of Q3:

client.html

```
<html>
<body>

<h1>Lab 7 Answer</h1>

<FORM ACTION="../server/server.php" method="POST">
    Enter the message: <input type="text" id="message" name="message" />
    <br/><br/>
    Enter the encryption key: <input type="text" id="DES_Encryption_Key"
name="DES_Encryption_Key" />
    <br/><br/>
    <button type="submit" onclick="DES_encryption()">Submit</button>
</table>

</FORM>

<script type="text/javascript"
src="http://titan.csit.rmit.edu.au/~e23700/Lab7/Demo1/des.js"></script>
<script type="text/javascript">

function DES_encryption() {

    var message = document.getElementById("message").value;

    var key = document.getElementById("DES_Encryption_Key").value;

    // javascript des encryption api
    var encrypted = javascript_des_encryption(key, message);

    document.getElementById("message").value = encrypted;

    return false;
}

</script>

</body>
</html>
```

server.php

```
<?php

include('des.php');

?>

<html>
<body>

<?php
```

```
//Receive user input from client side  
$message = $_POST['message'];
```

```
//set up a key by yourself  
$key = "this is the key";
```

```
//decrypt the received message using the key and PHP des decryption AIP  
$recovered_message = php_des_decryption($key, $message);
```

```
echo "Received encrypted Message: " . $message . "<br/><br/>";
```

```
echo "Decryption key: " . $key . "<br/><br/>";
```

```
echo "Recovered plaintext message: " . $recovered_message . "<br/><br/>";
```

```
//access to database/database.txt  
$file = fopen("../database/database.txt", "a");  
//insert this user into the users.txt file  
fwrite($file, $recovered_message . "\n");  
//close the "$file"  
fclose($file);
```

```
echo "The recovered message has been added to the ../database/database.txt";
```

```
?>
```

```
</body>  
</html>
```