File encryption & decryption using openSSL library

Build a solution to use (Open-SLL Library) to encrypt & decrypt files

❓ Solution Scenario

1- Allow user to select any file existing on his computer.
2- Show details (file name, file size, file extension) of the selected file on the application's main window.
3- Allow user to do the following operations "using OpenSSL library" on the selected file:
 a. Encrypt: allow user to encrypt the plain file using :
  i. AES "Advanced Encryption Standard" algorithm
  ii. 256 bits key size
  iii. CBC mode
 b. Decrypt: allow user to retrieve the plain file from the encrypted one.
4- Allow user to select the name and location before saving the encrypted/decrypted file.

Requirements

Show Details Of File In Main Window

DESCRIPTION
Show details (file name, file size, file extension) of the selected file on the applicatio...

Using OpenSSL library

DESCRIPTION
Encrypt & Decrypt (AES-256-CBC)

Saving File After Process

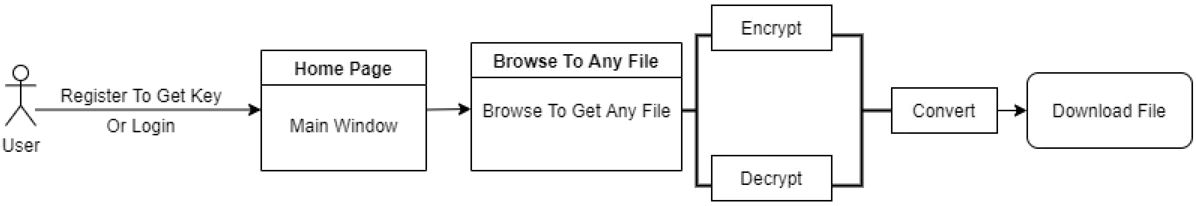
DESCRIPTION
before saving the encrypted/decrypted text file.

💡 *Here's what I have done*

- Application has simple authentication system with middleware.
- User can browse any file and upload it.
- User can click on load button on main window to get file name, file size in kB and extension.
- Application provide 256 key base key for each user when register for first time.
- Case of 256 key base key for each user to provide level of security if any security issues happens, Only one user affected by attack not all of content when using public key.
- There is a Function to take plain text and encrypt it to get Cipher text based on (AES-256-CBC) with user logged key.
- There is a function to take Cipher text version and decrypt to plain text based on (AES-256-CBC) with user logged key.
- User can download text file (Encrypted or Decrypted) after process process.

Technical Details

💹 Flow Chart For Solution

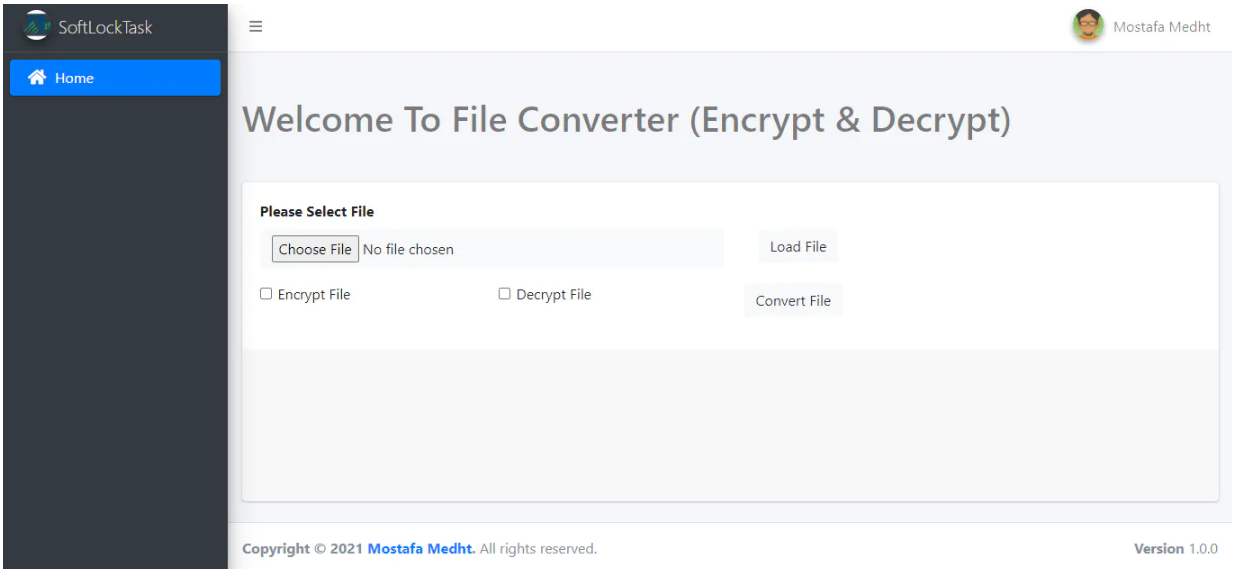


📝 Technical Details

- Building authentication system to generate special (256-key base) for each user.
- Generate private key for each user make this solution more secure in case of (leak of information)

```
base64_encode(openssl_random_pseudo_bytes(256));
```

- After login, Redirect to home page (Main Window).



Welcome To File Converter (Encrypt & Decrypt)

Please Select File

Choose File No file chosen

Load File

□ Encrypt File

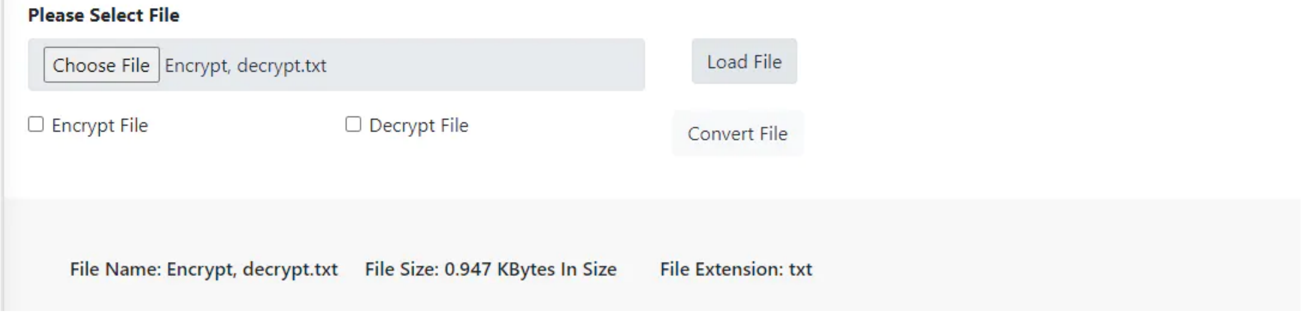
□ Decrypt File

Convert File

Copyright © 2021 Mostafa Medht. All rights reserved.

Version 1.0.0

- Click on (choose file) button to browse any file from your computer.
- After upload file, Click (load) button to get file info (name, size in KB, extension).



Please Select File

Choose File Encrypt, decrypt.txt

Load File

□ Encrypt File

□ Decrypt File

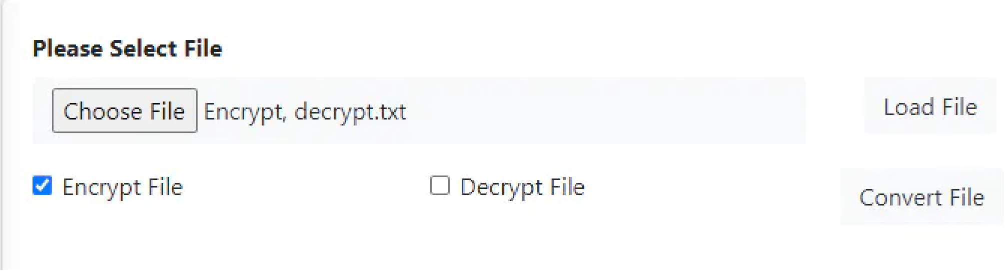
Convert File

File Name: Encrypt, decrypt.txt File Size: 0.947 KBytes In Size File Extension: txt

- Load button run JavaScript function to get file info using FileReader() API.

```
var file = input.files[0];
var extention = file.name.split('.').pop();
addPara("\tFile Name: " + file.name +
        "\tFile Size: " + (file.size)/1000 + " KBytes In Size "
        + "\tFile Extension: " + extention);
```

- Select (encrypt or decrypt) check box then click convert button.



Please Select File

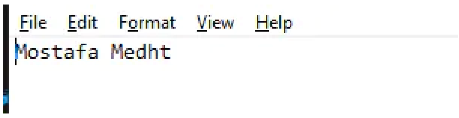
Choose File Encrypt, decrypt.txt

Load File

☑ Encrypt File

□ Decrypt File

Convert File



Mostafa Medht

- Convert button has event handler with jQuery to call Ajax request to DocumentController functions filtered by check box selected or checked (encrypt or decrypt).

```
$('#convert').on('click', function name(e) {
            // Check If one Of Check Box Selected
            var validity = checkboxCheck();
            if (!validity) {
                return;
            } // chexk if check box valid value
            if($("#encrypt").is(":checked")){
                senAjaxRequest("{{ route('file.encrypt') }}")
            } // send ajax with encrypt route
            else
            {
                senAjaxRequest("{{ route('file.decrypt') }}")
            } // send ajax with deccrpt value

        }); // end of click event (Convert Button)
```

- Using Ajax to decrease resources usage.
- After receiving request, Controller process this request by dependency injection from Request Helper.

```
public function decrypt(Request $request)
```

- Controller function get content of file to temporary variable.

```
 $contents= file_get_contents($request->file);
```

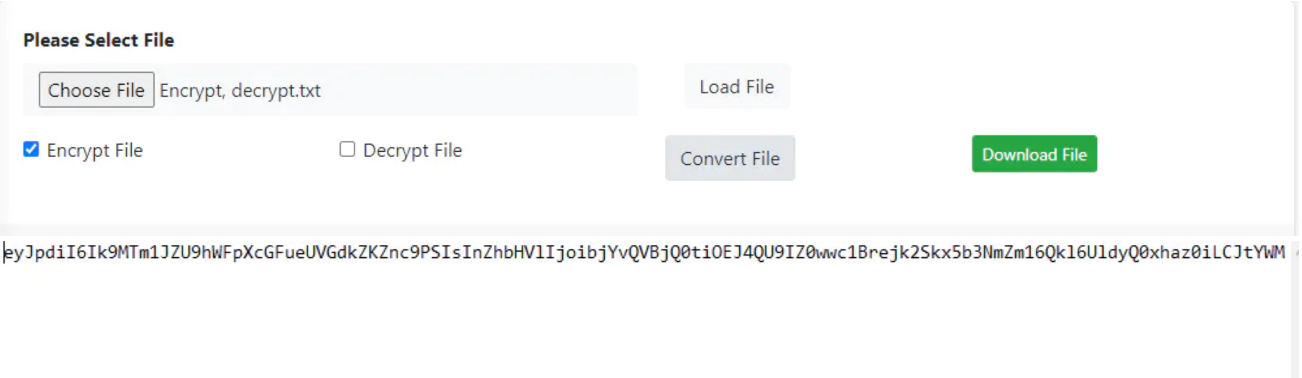
- Controller functions get user key from user table by Auth Facade.
- Controller functions get (encrypt or decrypt) functions using (EncryptDecryptTrait) built for this purpose.
- EncryptDecryptTrait has main (encrypt & decrypt) function body eg. (encryption or decryption algorithm (aes-256-cbc)).

```
trait EncryptDecryptTrait {

    public $ciphertext = '';
    public $cipher = "aes-256-cbc";

    public function encrypt($plainText, $key){
        global $cipher;
        return openssl_encrypt($plainText, $cipher, $key, $options=0, '', $tag);
    }

    function decrypt($cipherText, $key){
        global $cipher;
        return openssl_decrypt($cipherText, $cipher, $key, $options=0, '', '');
    }

}
```

- When using EncryptDecryptTrait functions take 2 parameters (plain text or chipper text & key for user).
- After process of controller function end, Return result in success function by ajax.
- Ajax success function put received data to text area then display download button.

```
success: function(response) {
    addTextToSave(response);
    $('#download').removeClass('d-none');
},
```

- Download button has event handler to set download attribute and get text from textarea to save it as file.



eyJpdiI6Ik9MTm1JZU9hWFpXcGFueUVGdkZKZnc9PSIsInZhbHVlIjoibjYvQVBjQ0tiOEJ4QU9IZ0wwc1Brejk2Skx5b3NmZm16Qkl6UldyQ0xhaz0iLCJtYWM

Summary and Conclusions

Technologies and Packages Used For This App

- **Technologies**
  - □ **Bootstrap (V 4.6)**
  - □ **JavaScript**
  - □ **jQuery (V 3.5)**
  - □ **Ajax**
  - □ **PHP**
  - □ **Laravel (V 7.3)**
- **Packages and Libraries**
  - □ **Admin LTE**
  - □ **FileReader() API**
  - □ **Open SSL Library Of PHP**
  - □ **Open SSL Library Of PHP**
  - □ **Download function help guide**