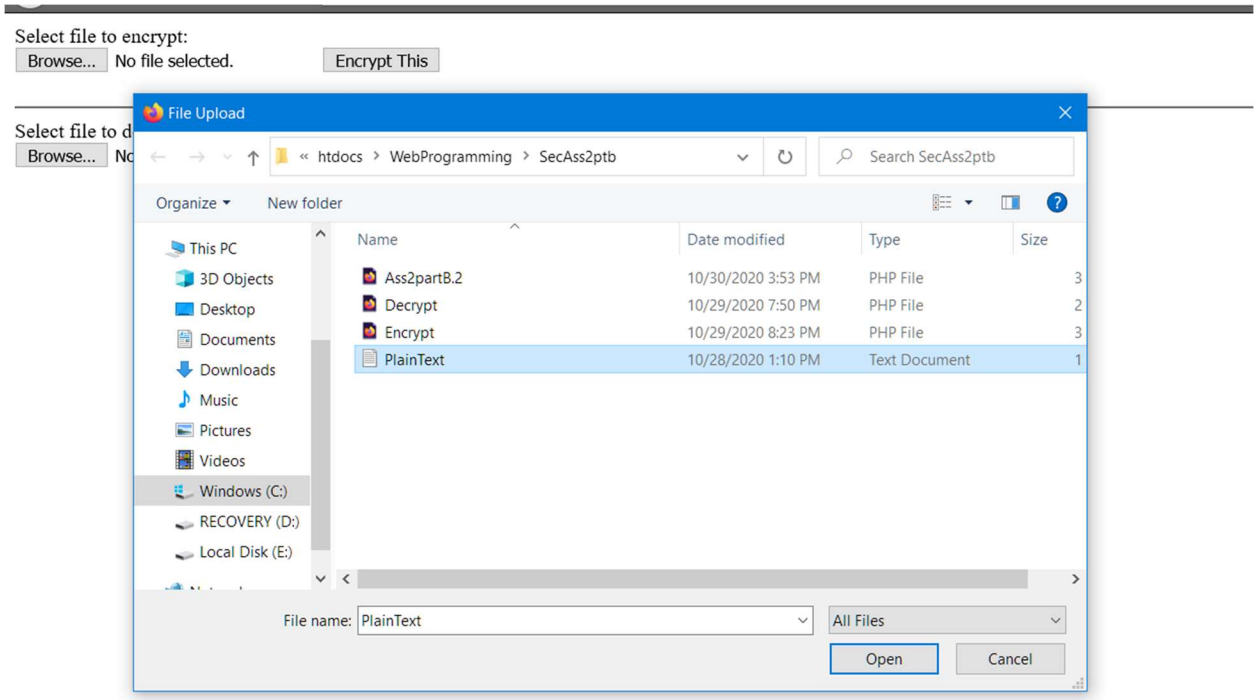
Scott Wickline

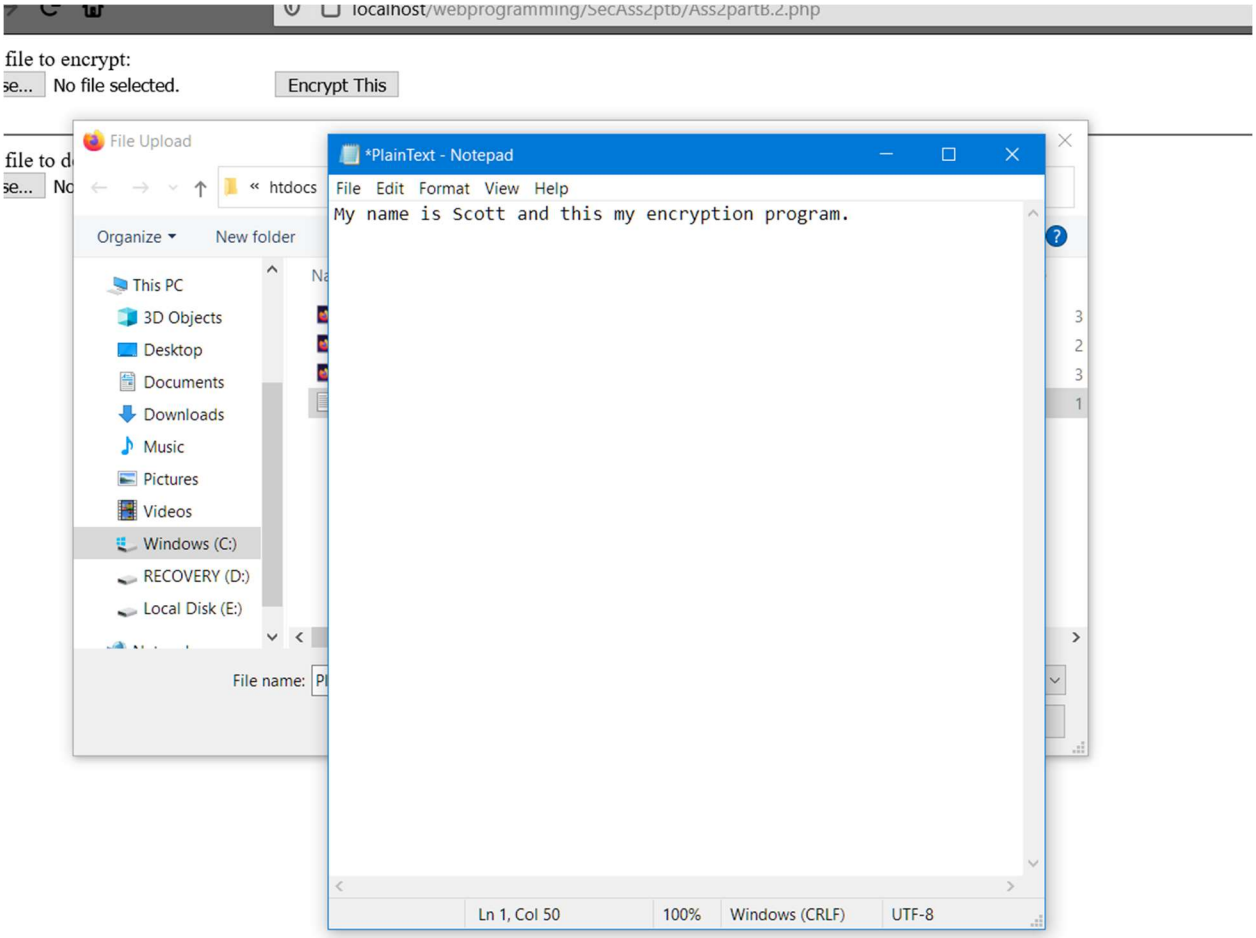
Assignment2 Part B

I chose PHP for my Encryption and Decryption program. I used the AES-256-CBC Algorithm.

This is where the user would open the page. The top section is form to select a file on the machine running the program.

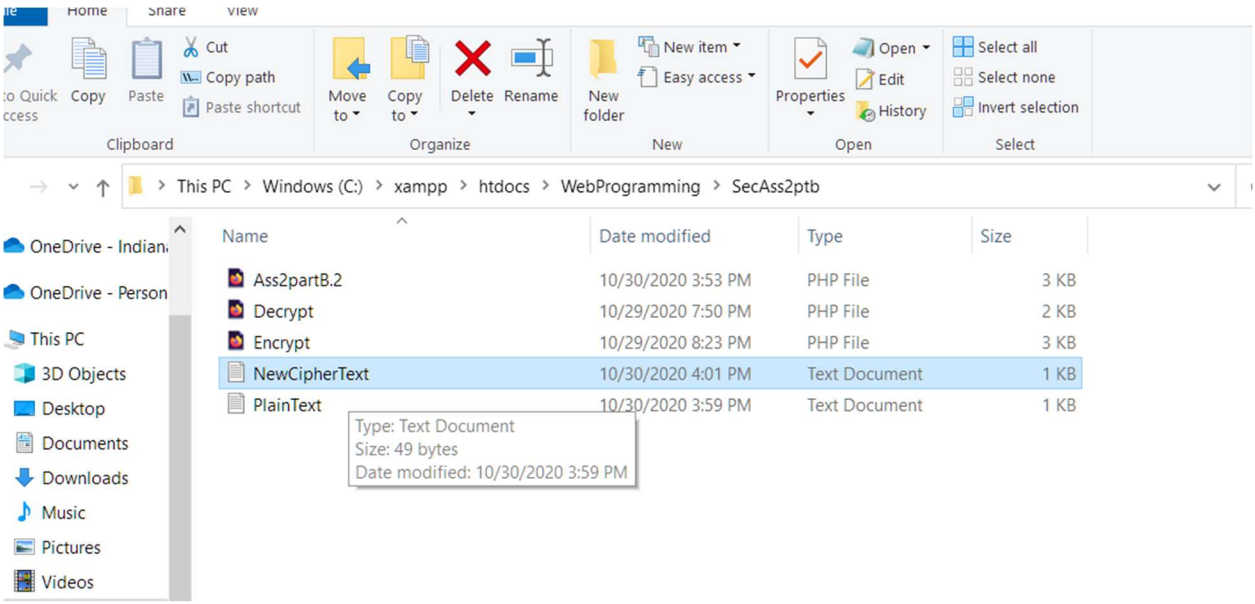


After Clicking browse File upload box opens where the user can select their file to encrypt. I selected the PlainText.txt.



Content of file before encryption.

Once chosen the file name will show in the form. Then click Encrypt This and a ciphertext will be created.



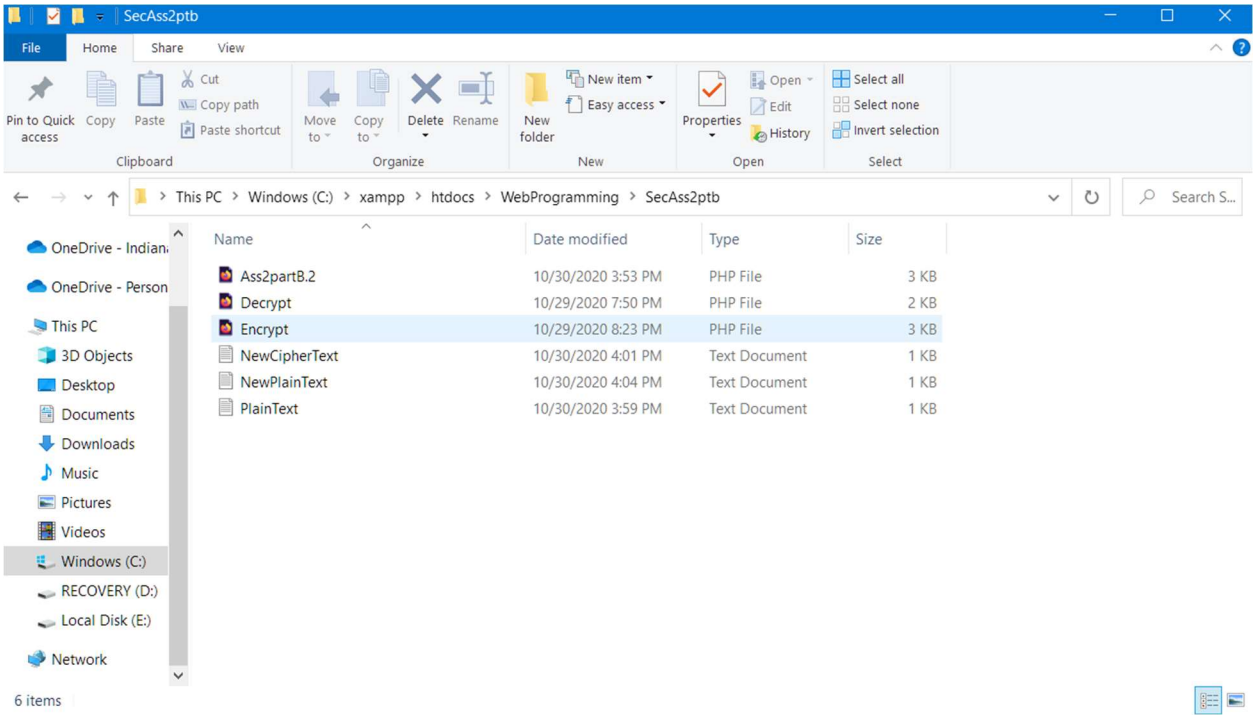
New CipherText.txt has appeared in the directory.

Content is the encrypted plain text from PlainText.txt.

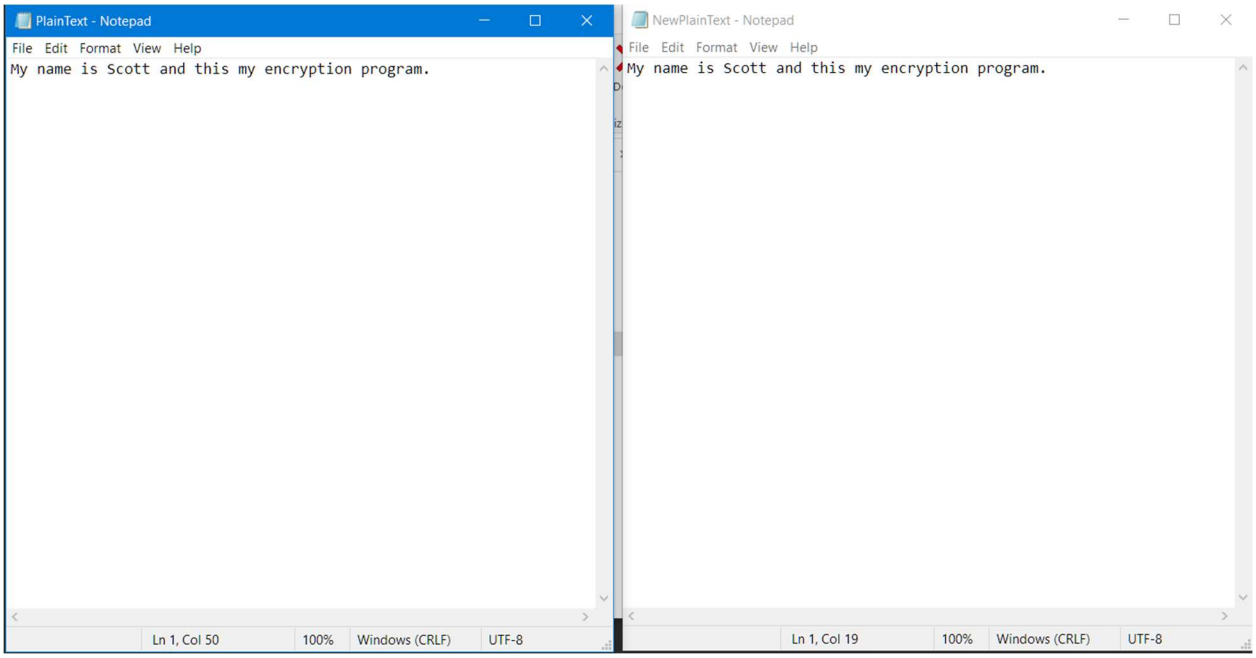
Select file to encrypt:
Browse... No file selected. Encrypt This

Select file to decrypt:
Browse... NewCipherText.txt Decrypt This

To decrypt select a file like before but use the lower browse button. Then select Decrypt This.



A new file named NewPlainText.txt should now have appeared and should contain the plain text from the original document.



The file NewPlainText contains the same message as Plaintext.txt.

```php
//This fucntion encrypts the plain text.
function EncryptThis($ClearTextData) {
    global $ENCRYPTION_KEY;
    global $ENCRYPTION_ALGORITHM;
    $EncryptionKey = base64_decode($ENCRYPTION_KEY);
    $InitializationVector  = openssl_random_pseudo_bytes(openssl_cipher_iv_length($ENCRYPTION_ALGORITHM));
    $EncryptedText = openssl_encrypt($ClearTextData, $ENCRYPTION_ALGORITHM, $EncryptionKey, 0, $InitializationVector);
    return base64_encode($EncryptedText . '::' . $InitializationVector);

}

// This function decrypts the cipher data.
function DecryptThis($CipherData) {

    global $ENCRYPTION_KEY;
    global $ENCRYPTION_ALGORITHM;
    $EncryptionKey = base64_decode($ENCRYPTION_KEY);
    list($Encrypted_Data, $InitializationVector ) = array_pad(explode('::', base64_decode($CipherData), 2), 2, null);
    return openssl_decrypt($Encrypted_Data, $ENCRYPTION_ALGORITHM, $EncryptionKey, 0, $InitializationVector);
}
```

These are my Encrypt and Decrypt functions. I used the openssl library in php.

```php
//and then decrypted.
if (!empty($_POST["ClearTextData"])) {

    $My_E_File = file_get_contents($_POST["ClearTextData"]) or die("Unable to open file!");
    $My_E_File = EncryptThis($My_E_File);
    file_put_contents("NewCipherText.txt", $My_E_File);

}
//Checks to see if POST Array is intinalized if so...
//POST is then copied and the target file is opened
//and then decrypted.
if (!empty($_POST["CipherData"])) {

    $My_D_File = file_get_contents($_POST['CipherData']) or die("Unable to open file!");
    $My_D_File = DecryptThis($My_D_File);
    file_put_contents("NewPlainText.txt", $My_D_File);

}
```

These two if statements check the POST array to make sure it's initialized. If so the POST array target file is opened and content copied as a string. That string is passed into the encryption function. Then encrypted/decrypted text is written to a new file In the directory.