Mini Project – Programming Laboratory 1

Project by:

Chandana Galgali – 16010422234

Mahek Thakkar – 16010422235

Problem Statement -

I Part:

You are given two functions, encrypt and decrypt, that perform encryption and decryption operations on a given message using a key and shift direction. The encrypt function takes a message, key, and shift direction as input and returns the encrypted message. The decrypt function takes an encrypted message, key, and shift direction as input and returns the decrypted message.

II Part:

The problem is to implement data encryption and decryption using XOR and AES algorithms. The program should provide options for the user to choose between XOR encryption and decryption or AES encryption and decryption. The XOR encryption and decryption should take a data file and an encryption key as input, while the AES encryption and decryption should take a data file, and a password as input. The program should perform the encryption and decryption operations based on the user's choice and display the appropriate output.

Before using the second program, the user needs to have three libraries installed using 'pip'. Following are the commands to run before executing the program (which is just a one-time install and the user can continue to use it later on without running these commands again):

- `pip install os`
- `pip install pyAesCrypt`

- The *os module* in Python provides a way to interact with the operating system. It offers various functions for performing operating system-related tasks, such as file and directory operations, process management, environment variables, and more.

- The *pyAesCrypt module* is a Python library that provides AES encryption and decryption functionality. AES (Advanced Encryption Standard) is a symmetric encryption algorithm widely used for securing data.

1. Start the I program.

2. Prompt the user to enter the message to encrypt/decrypt.

```
Enter the message to encrypt/decrypt:
```

3. Read the message from the user.

```
Enter the message to encrypt/decrypt: Hello everyone! This is the...
```

4. Prompt the user to enter a positive integer key.

```
Enter the message to encrypt/decrypt: Hello everyone! This is the first part of our code, it encrypts and decrypts text.
Enter the key (a positive integer):
```

5. Read the key from the user.

```
Enter the message to encrypt/decrypt: Hello everyone! This is the first part of our code, it encrypts and decrypts text.
Enter the key (a positive integer): 4
```

6. Prompt the user to enter the shift direction (1 for right shift, -1 for left shift).

```
Enter the message to encrypt/decrypt: Hello everyone! This is the first part of our code, it encrypts and decrypts text.
Enter the key (a positive integer): 4
Enter the shift direction (1 for right shift, -1 for left shift):
```

7. Read the shift direction from the user.

```
Enter the message to encrypt/decrypt: Hello everyone! This is the first part of our code, it encrypts and decrypts text.
Enter the key (a positive integer): 4
Enter the shift direction (1 for right shift, -1 for left shift): 1
```

8. Print the encrypted message.

```
Enter the message to encrypt/decrypt: Hello everyone! This is the first part of our code, it encrypts and decrypts text.
Enter the key (a positive integer): 4
Enter the shift direction (1 for right shift, -1 for left shift): 1
Encrypted message: Lipps izivcsri! Xlmw mw xli jmvwx tevx sj syv gshi, mx irgvctxw erh higvctxw xibx.
```

9. Print the decrypted message.

```
Enter the message to encrypt/decrypt: Hello everyone! This is the first part of our code, it encrypts and decrypts text.
Enter the key (a positive integer): 4
Enter the shift direction (1 for right shift, -1 for left shift): 1
Encrypted message: Lipps izivcsri! Xlmw mw xli jmvwx tevx sj syv gshi, mx irgvctxw erh higvctxw xibx.
Decrypted message: Hello everyone! This is the first part of our code, it encrypts and decrypts text.
```

10. End the program.

1. Start the II program.

2. Display a menu with 2 options:
XOR Encryption and Decryption, and AES Encryption and Decryption.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
```

3. Prompt the user to enter their choice.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice:
```

If the user chooses XOR Encryption and Decryption:

4. Display sub-menu options for encryption and decryption.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 1
1. Press 1 for Encryption
2. Press 2 for Decryption
```

5. Prompt the user to choose between encryption and decryption.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 1
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter your choice:
```

If the user chooses encryption:

6. Prompt the user to enter the path of the data file.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 1
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter your choice: 1
Enter path of data:
```

7. Prompt the user to enter the encryption key.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 1
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter your choice: 1
Enter path of data: /content/sample-1.jpg
Enter Key for encryption of data:
```

8. Display a success message.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 1
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter your choice: 1
Enter path of data: /content/sample-1.jpg
Enter Key for encryption of data: 5
The path of file:  /content/sample-1.jpg
Key for encryption:  5
Encryption Done Successfully!
```

If the user chooses decryption:

6. Prompt the user to enter the path of the data file.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 1
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter your choice: 2
Enter path of data:
```

7. Prompt the user to enter the decryption key.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 1
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter your choice: 2
Enter path of data: /content/sample-1.jpg
**************************************************
Note: Encryption key and Decryption key must be the same!
**************************************************
Enter Key for encryption of data:
```

8. Display a success message.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 1
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter your choice: 2
Enter path of data: /content/sample-1.jpg
**********************************************************
Note: Encryption key and Decryption key must be the same!
**********************************************************
Enter Key for encryption of data: 5
The path of file:  /content/sample-1.jpg
Key for Decryption:  5
Decryption Done Successfully!
```

If the user chooses AES Encryption and Decryption:

4. Display sub-menu options for encryption and decryption.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 2
1. Press 1 for Encryption
2. Press 2 for Decryption
```

5. Prompt the user to choose between encryption and decryption.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 2
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter the Choice:
```

If the user chooses encryption:

6. Prompt the user to enter the path of the data file.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 2
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter the Choice: 1
Enter the file location with extension:
```

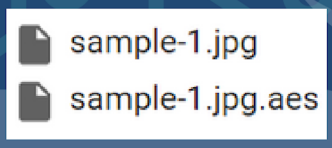
7. Prompt the user to enter a password for encryption.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 2
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter the Choice: 1
Enter the file location with extension:/content/sample-1.jpg
Enter the password:
```

8. Display a success message.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 2
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter the Choice: 1
Enter the file location with extension:/content/sample-1.jpg
Enter the password: 1234
Encryption Done Succcesfully!
```

Write the encrypted data to a new file with the ".aes" extension.



If the user chooses decryption:

6. Prompt the user to enter the path of the encrypted file.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 2
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter the Choice: 2
Enter the file location with extension:
```

7. Prompt the user to enter the password for decryption.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 2
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter the Choice: 2
Enter the file location with extension:/content/sample-1.jpg.aes
Enter the password:
```

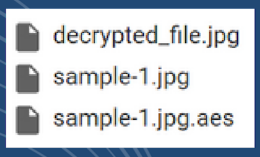
8. Prompt the user to enter the name of the decrypted file.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 2
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter the Choice: 2
Enter the file location with extension:/content/sample-1.jpg.aes
Enter the password: 1234
364055
Decrypted file name (Make sure to put the extension of the format you want your decrypted file in!):
```

9. Display a success message.

```
1. Data XOR Encryption and Decryption
2. Data AES Encryption and Decryption
Enter your choice: 2
1. Press 1 for Encryption
2. Press 2 for Decryption
Enter the Choice: 2
Enter the file location with extension:/content/sample-1.jpg.aes
Enter the password: 1234
364055
Decrypted file name (Make sure to put the extension of the format you want your decrypted file in!):decrypted_file.jpg
Decryption Done Succcesfully!
<ipython-input-34-3ec0327bf074>:72: DeprecationWarning: inputLength parameter is no longer used, and might be removed in a future version
  pyAesCrypt.decryptStream(fIn, fOut, password, bufferSize, encFileSize)  # Decrypt the file using AES decryption
```

Write the decrypted data to the specified file.



End the program.