Workshop 4 – Symmetric Encryption

**Task**

**For this task you will write an application of the following symmetric encryption algorithm using cryptographic primitives of the cryptography.io Python module:**

* **AES-256-CBC**

**Upon identifying the procedure for using the Python library for the AES-CBC cryptographic primitive, you are to write an encryption and decryption program. Both these programs should be interactive i.e., receive user input i.e., a *passphrase* and a *filename*.**

**The user message should be padded with padding bits to make it a multiple of 16 before it is encrypted. A random IV should be generated. The IV and the padding character used to pad the message should be appended to the encrypted message and then stored in a text file in the same directory (filename was provided by the user). The decryption program asks the user for the filename and the passphrase. It then extracts the IV, padding character and cipher from the file. Once the message is decrypted, the padding bits are removed and the original message is displayed to the user. Refer to the flow charts on the next pages.**

**Submission Requirements**

**Your code must comprise the following components:**

* **Prompt for user input (1)**
* **Generate a random IV (1)**
* **Pad the message (2)**
* **Encrypt the message using AES256-CBC mode (2)**
* **Add the IV, the character used for padding, to cipher and store in a file (1)**
* **Extract the IV, decrypt the message, remove the padding and display the original message (3)**

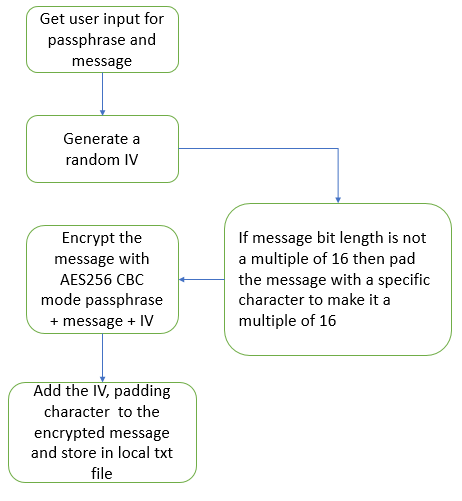
**You must submit the following:**

* **The source code for your implementation**
* **Documentation (2 pages maximum) explaining your implementation**
* **Instructions for running your program to meet the objectives**

**Program Flow chart**

**Encryption Program:**

.



**Decryption Program:**

