Week 6 Lab

Task 1: Understand the Components  
1. Analyze the padding\_oracle function. How does it determine if padding is valid?

The padding\_oracle function checks if padding is good or bad. First, it looks at the message length. The message must be exactly 16 bytes, 32 bytes, 48 bytes, etc. If not, it says "bad padding". Next, it takes the first 16 bytes as the IV. It takes the rest as the secret message. Then it decrypts the secret message using AES. After that, it tries to remove padding bytes. If removing padding works, it says "good padding". If removing padding fails, it says "bad padding".  
  
2. What is the purpose of the IV in CBC mode?   
The IV (initialization vector) is like a starting number for encryption. In CBC mode, each block depends on the block before it. The first block has no block before it. So, the IV acts as the "block before" for the first block. During decryption, the IV is XORed with the first decrypted block. This outputs the original first block of text. The IV must be the same for encryption and decryption to work.  
  
3. Why does the ciphertext need to be a multiple of the block size?  
AES only works with complete 16-byte blocks. It cannot handle 15 bytes or 17 bytes. The math inside AES needs exactly 16 bytes. CBC mode also needs complete blocks. Each block connects to the next block. If we have incomplete blocks, the connection breaks. Padding makes sure there is always complete blocks.

Task 2: Implement Block Splitting

Task 3: Implement Single Block Decryption  
Task 4: Implement Full Attack  
Task 5. Implement Plaintext Decoding  
  
The implementation for these tasks is provided in the following python file -> main.py (and its dependency folders - .idea and .venv).