Programming Assignment 2.

In this project you will implement two encryption/decryption systems, one using AES in CBC mode and another using AES in counter mode (CTR). In both cases the 16-byte encryption IV is chosen at random and is prepended to the ciphertext. For CBC encryption we use the PKCS5 padding scheme.

In the following questions you are given an AES key and a ciphertext (both are hex encoded) and your goal is to recover the plaintext.

For an implementation of AES you may use an existing crypto library. While it is fine to use the built-in AES functions, we ask you implement CBC and CTR modes yourself. Please submit your code with a document which covers your code explanation.

Question 1
CBC key: 140b41b22a29beb4061bda66b6747e14
CBC Ciphertext 1:
4ca00ff4c898d61e1edbf1800618fb2828a226d160dad07883d04e008a7897ee2e4b7465d5290d0c0e6c6822236e1daafb94ffe0c5da05d9476be028ad7c1d81

Question 2
CBC key: 140b41b22a29beb4061bda66b6747e14
CBC Ciphertext 2:
5b68629feb8606f9a6667670b75b38a5b4832d0f26e1ab7da33249de7d4afc48e713ac646ace36e872ad5fb8a512428a6e21364b0c374df45503473c5242a253

Question 3
CTR key: 36f18357be4dbd77f050515c73fcf9f2
CTR Ciphertext 1:
69dda8455c7dd4254bf353b773304eec0ec7702330098ce7f7520d1cbbb20fc388d1b0adb5054dbd7370849dbf0b88d393f252e764f1f5f7ad97ef79d59ce29f5f51eeca32eabedd9afa9329

Question 4
CTR key: 36f18357be4dbd77f050515c73fcf9f2
CTR Ciphertext 2:
770b80259ec33beb2561358a9f2dc617e46218c0a53cbeca695ae45faa8952aa0e311bde9d4e01726d3184c34451