**Question 1**

Assume an honest user wants to send an 8-bit integer to their bank indicating how much money should be transferred to the bank account of an attacker. The user uses **CTR-mode** encryption based on a block cipher F with 8-bit block length. (Yes, this is a made-up example.) The attacker knows that the amount of money the user wants to transfer is exactly **$16**, and has compromised a router between the user and the back. The attacker receives the ciphertext 10111100 01100001 (in binary) from the user. What ciphertext should the attacker forward to the bank to initiate a transfer of exactly **$32**? (Recall that CTR-mode decryption of a ciphertext *c*0,*c*1 using key *k* is done by outputting *c*1⊕*Fk*(*c*0+1).)10111100 01010001

**Question 2**

Assume CTR-mode encryption with PKCS #5 padding and a block cipher with 8-byte block length. Say a 4-byte message is encrypted, resulting in ciphertext 0x00 01 02 03 04 05 06 07 00 01 02 03 04 05 06 07. Which of the following ciphertexts will NOT yield an error upon decryption?

0x00 01 02 03 04 05 06 07 00 01 02 03 05 05 06 07

0x00 01 02 03 04 05 06 07 00 01 02 03 04 05 07 07

0x00 01 02 03 04 05 06 07 00 01 02 04 04 05 06 07

0x00 01 02 03 04 05 06 07 00 01 02 03 04 05 06 F7