Poison IV

Problem: Can you give me the IV to make the current plain text that is encrypted with AES to decrypt to the second plain text. Send the IV needed to chain the plain text to nc 192.168.3.5 64444

Given:

Original plain text: Pass: sup3r31337. Don't loose it!

Cipher text:
4f3a0e1791e8c8e5fefe93f50df4d8061fee884bcc5ea90503b6ac1422bda2b2b7e6a975bfc555f44f7dbcc30aa1fd5e

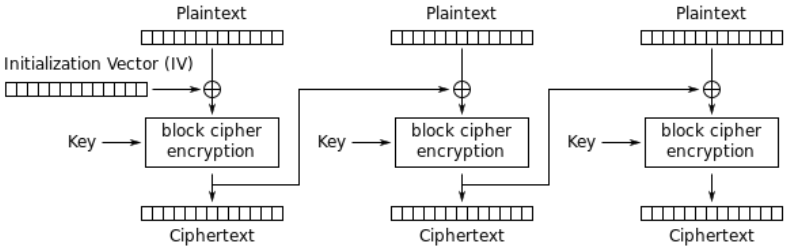
IV: 19a9d10c3b155b55982a54439cb05dce

Target plain text after decryption: Pass: notAs3cre7. Don't loose it!

Hint: Study up on AES CBC first block byte swapping

Steps:

1) Understanding aes-cbc. Aes is a type of encryption that encrypts blocks of data. To learn more about aes and the different modes at https://en.wikipedia.org/wiki/Advanced_Encryption_Standard



Cipher Block Chaining (CBC) mode encryption

AES is a block cipher, which means that plaintext is split into blocks: every block is encoded with an encryption key of an equal length (128, 192 or 256 bits in case of AES). By itself, a block cipher is only suitable for secure transmission of one block; in order to encode larger amounts of data, various modes of operation were introduced. CBC (Cipher Block Chaining) is one of such modes. To encrypt a block in CBC mode each block's plaintext is XORed with the preceding block's ciphertext (or IV for the first block), then encoded with a chosen algorithm (AES in our case). CBC is widely-used, but because of its properties it's vulnerable to byte-flipping attacks: when you change a byte in a block's ciphertext, the byte in the same position of the next block's plaintext gets changed because of the XOR operation.

2) In the problem, we are given:
(a) the original plain text “Pass: sup3r31337. Don't loose it!”.

(b) the cipher text
“4f3a0e1791e8c8e5fefe93f50df4d8061fee884bcc5ea90503b6ac1422bda2b2b7e6a975bfc555f44f7dbcc30aa1fd5e”
(c) The initial vector IV “19a9d10c3b155b55982a54439cb05dce”

We don't know the key. But, we want to find a malicious IV' such as the decryption with the malicious IV will produce an altered plain text “Pass: notAs3cre7. Don't loose it!”

3) The way we start to get our answer is by using the computation used by AES CBC of encrypting and decrypting the first block of message (16bytes).
Encryption: C = Enc(IV xor M)
Decryption: M = IV xor Dec(C)

If we use a malicious IV' in decription, then we get M' = IV' xor Dec(C).
Here, we find an equation Dec(C) = IV xor M = IV' xor M'
Hence, IV' = IV xor M xor M'

The notations are
C=cipher text
IV=initial vector
IV’=malicious initial vector to produce our altered plain text after decryption
M=original plain text
M’ = altered plan text

4) Now, make a script to calculate IV' = IV xor M xor M'. Note that we only need the first block (16 bytes) of M and M' with IV.
IV is “19a9d10c3b155b55982a54439cb05dce”.
M is “Pass: sup3r31337”.
M' is "Pass: notAs3cre7”.