**Applied Cryptography (UE20CS314)**

**Padding Oracle Lab**

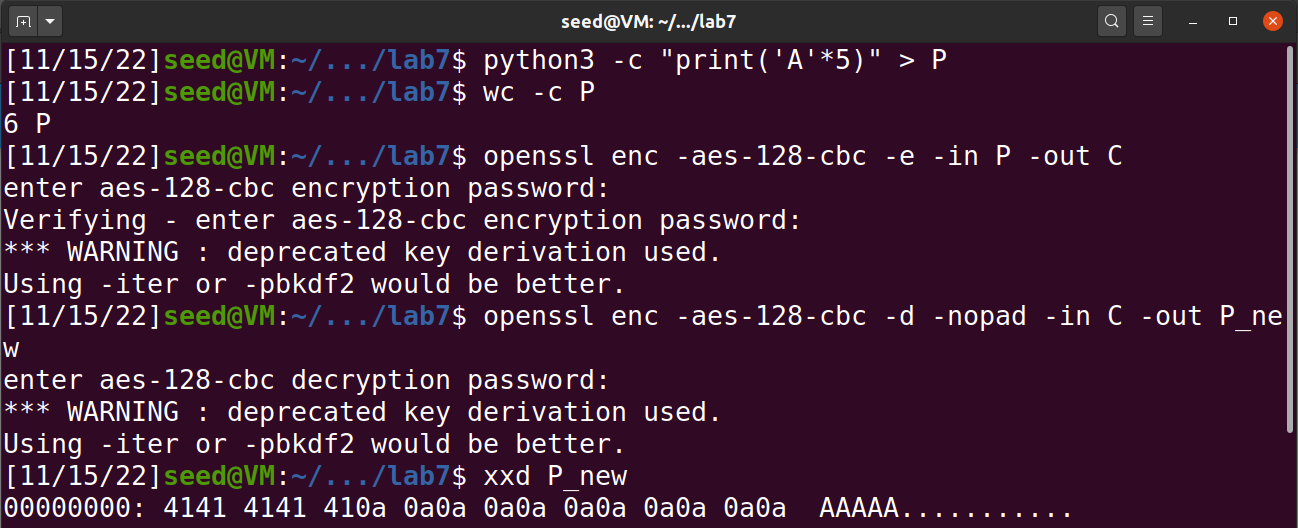
Name: Vishwa Mehul Mehta

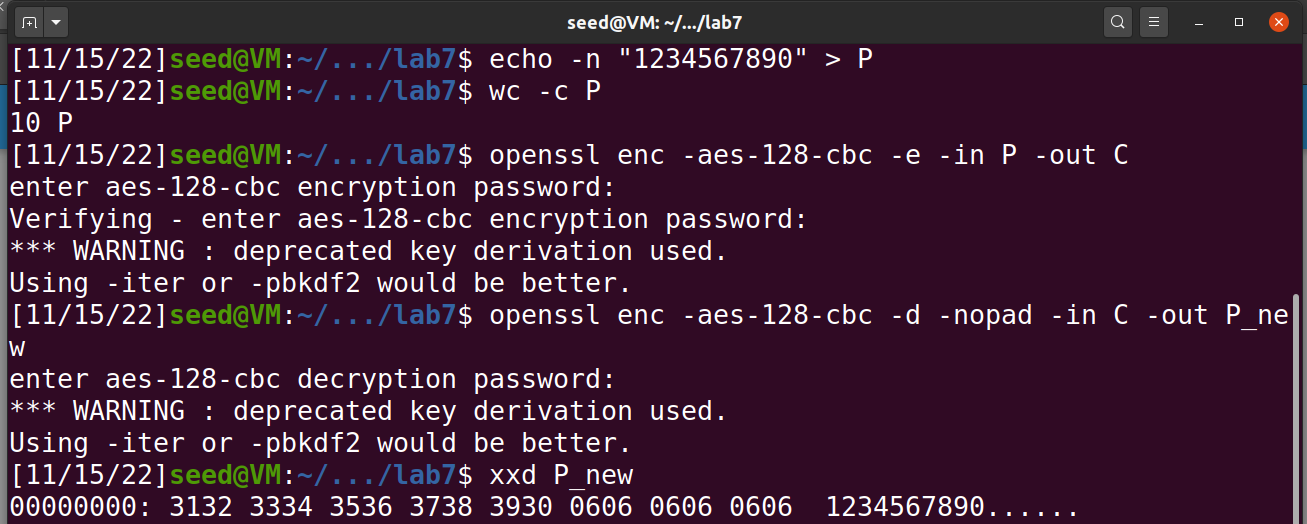
SRN: PES2UG20CS389

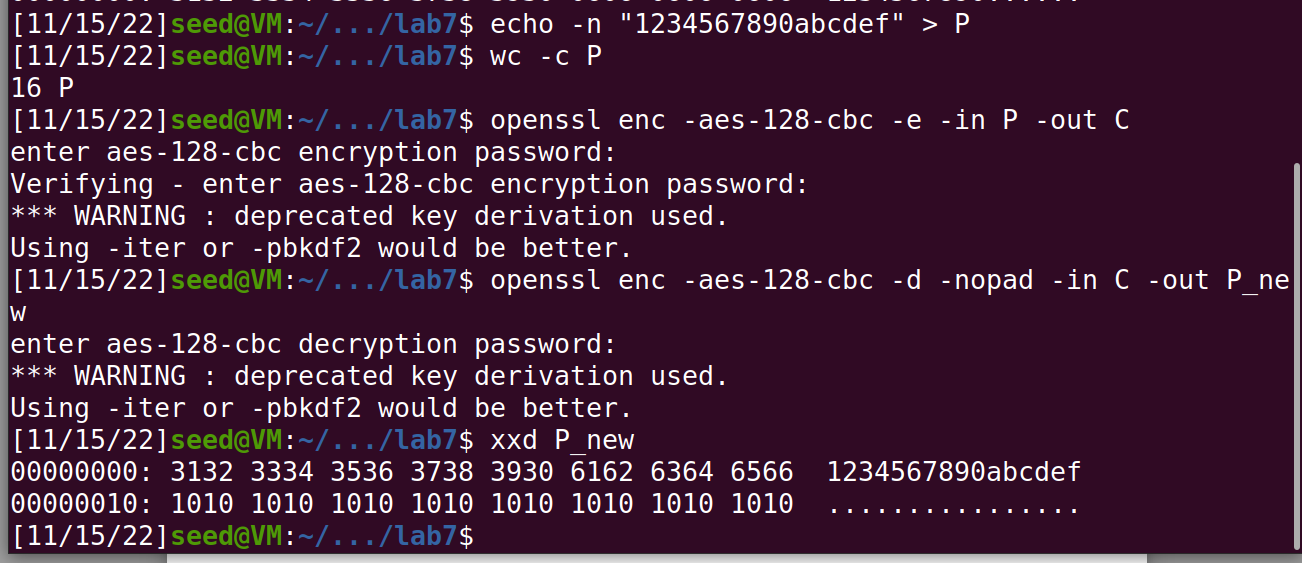
Section: F

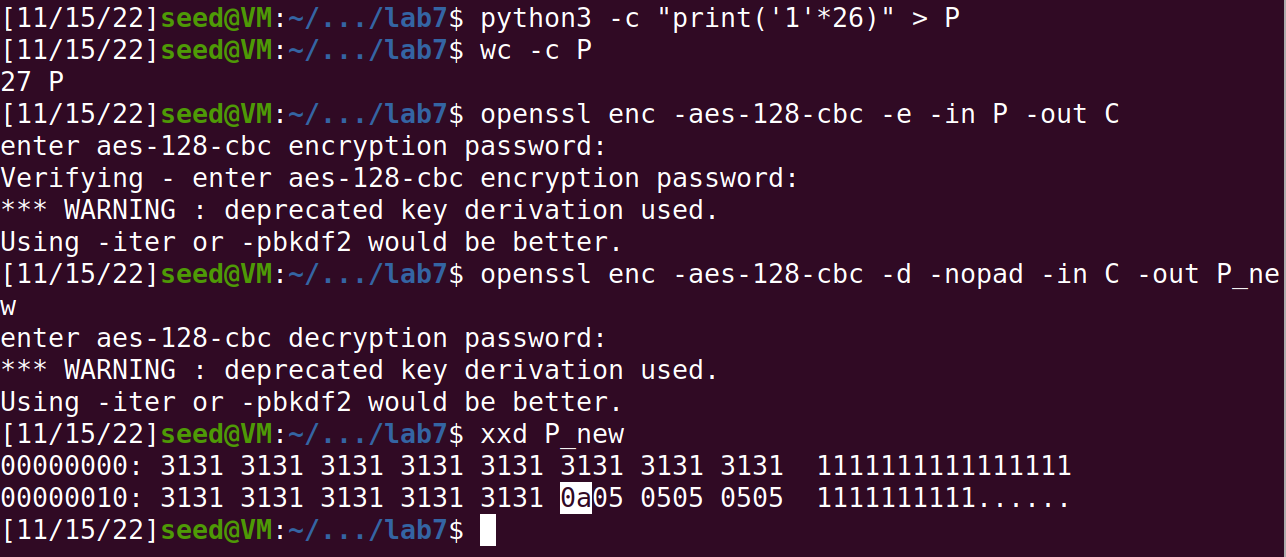
Task 1:

Screenshot:







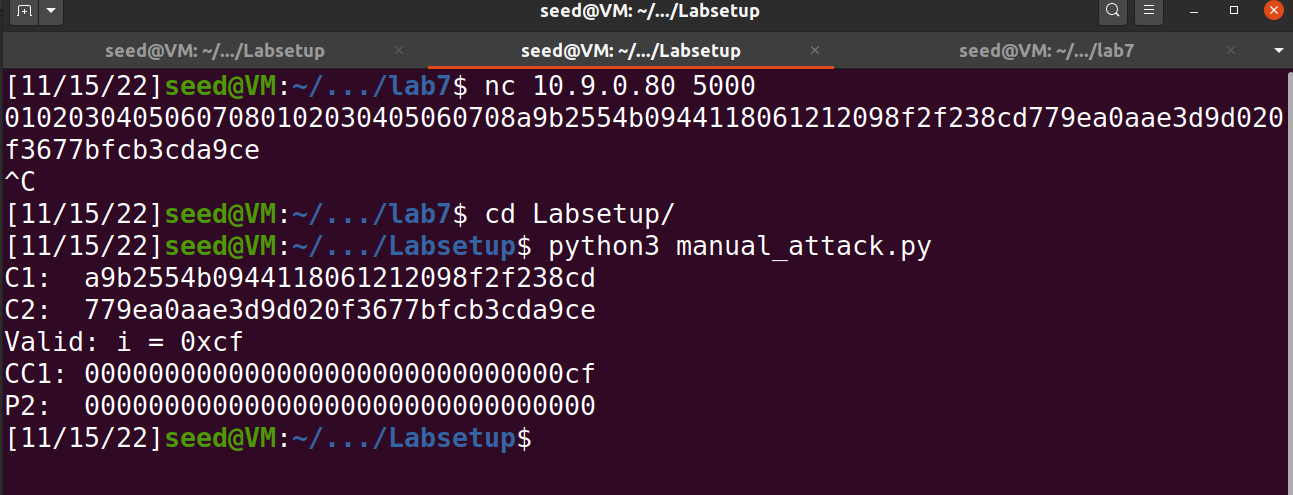


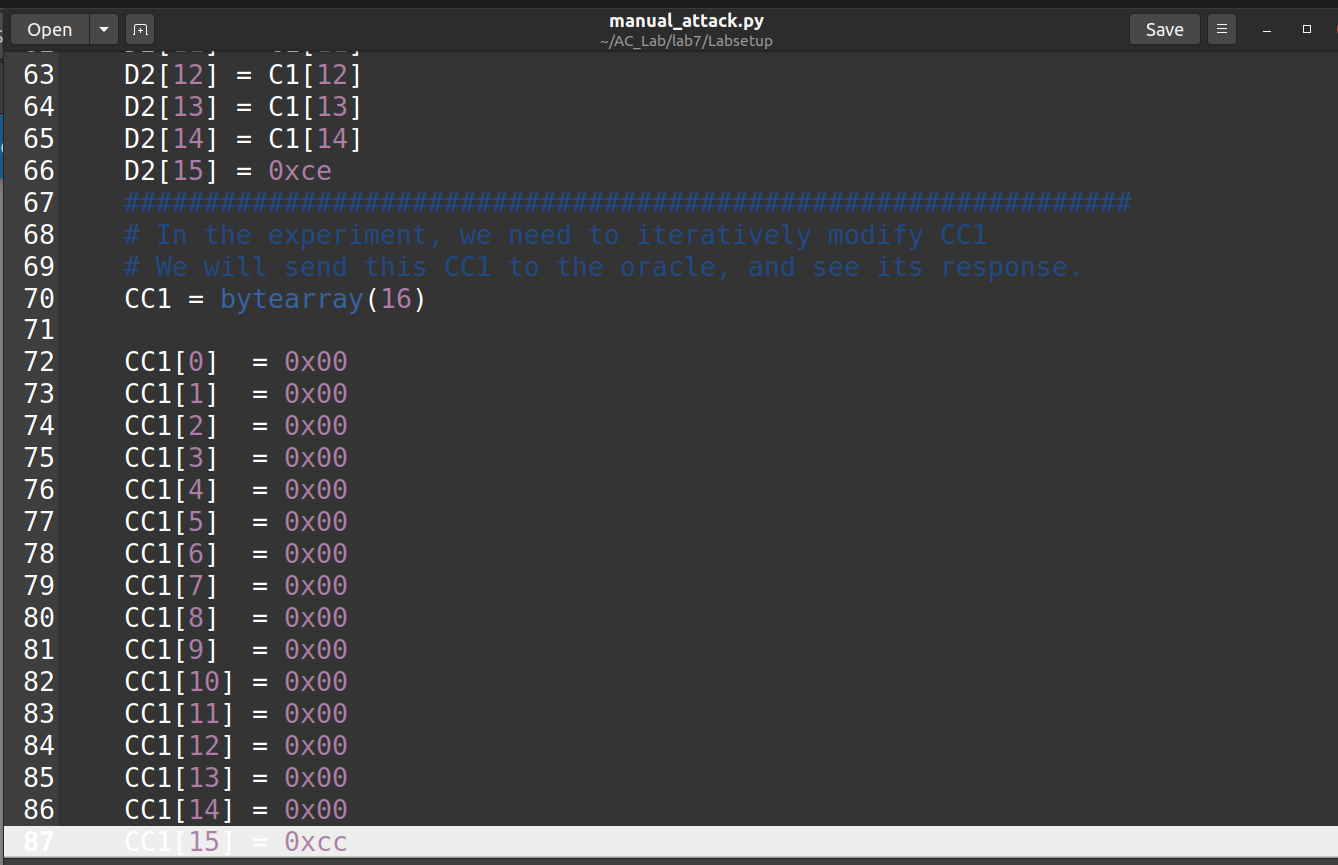
Observation:

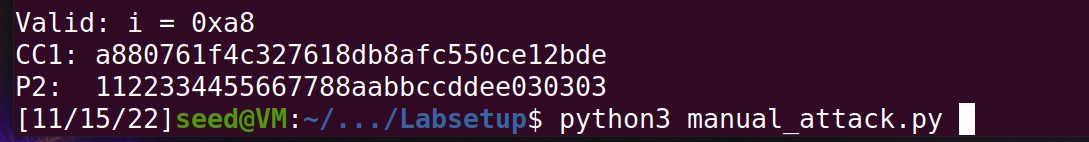
The padding for 5, 10, 16 and 27 bit is “0a”, “06”, “10” and “05” respectively. This shows that the padding value is equal to length of the characters mod 16.

Task 2:

Screenshot:



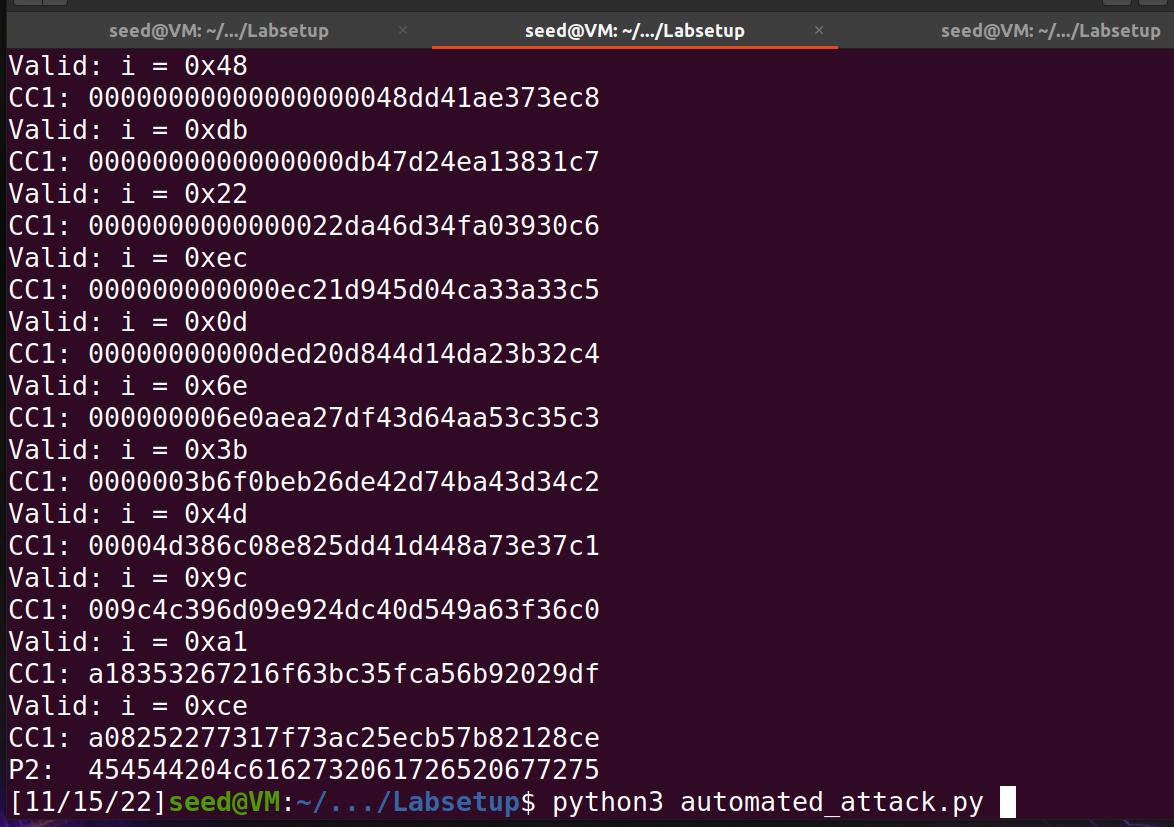




Observation:

After performing the changes manually we have got the value of the plaintext = 12233445566778811223344556677881122334455667788aabbccddee030303

Task 3:

Screenshot: 

Observation:

We now do the same process with port number 6000 and run the automated attack to find the final plaintext.