**APPLIED CRYPTOGRAPHY**

NAME: VISHWAS M

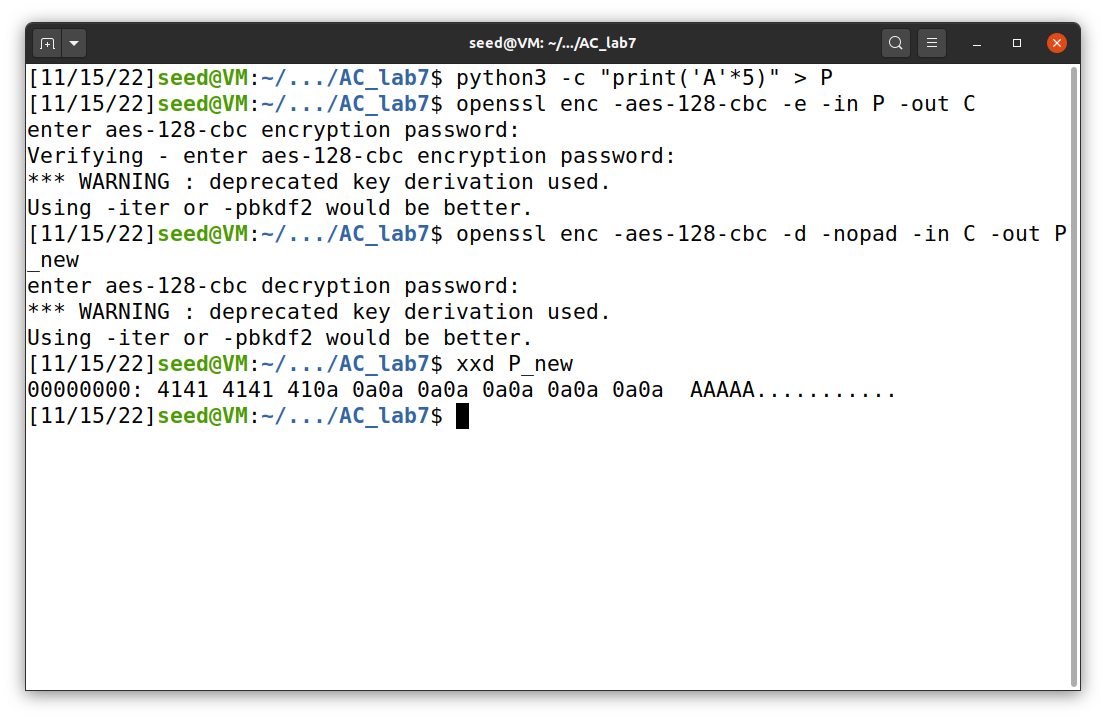
SRN: PES2UG20CS390

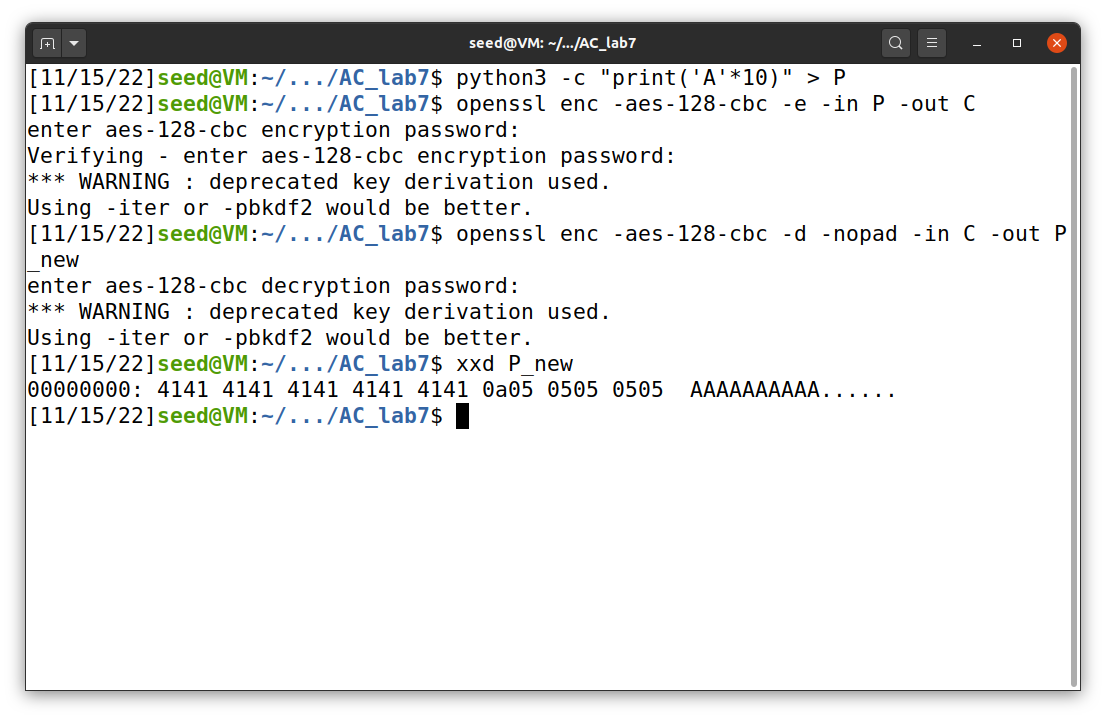
SEC: F

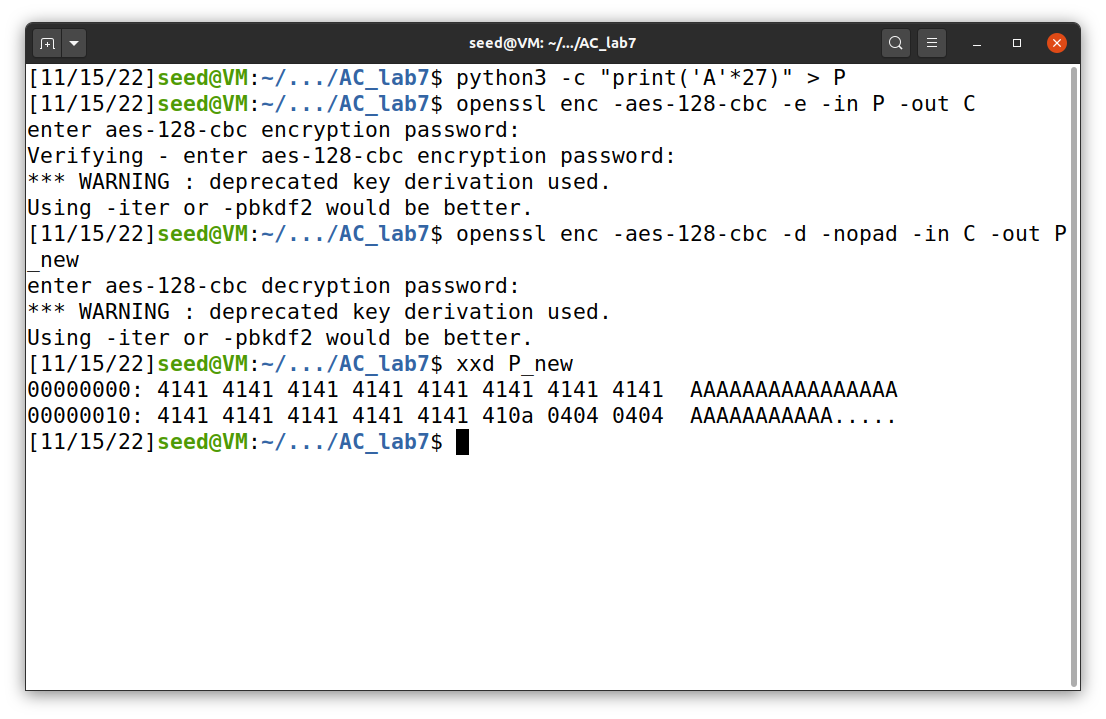
LAB: 7

TASK 1: Getting Familiar with Padding

1. Length 5:



1. Length 10:
2. Length 27:

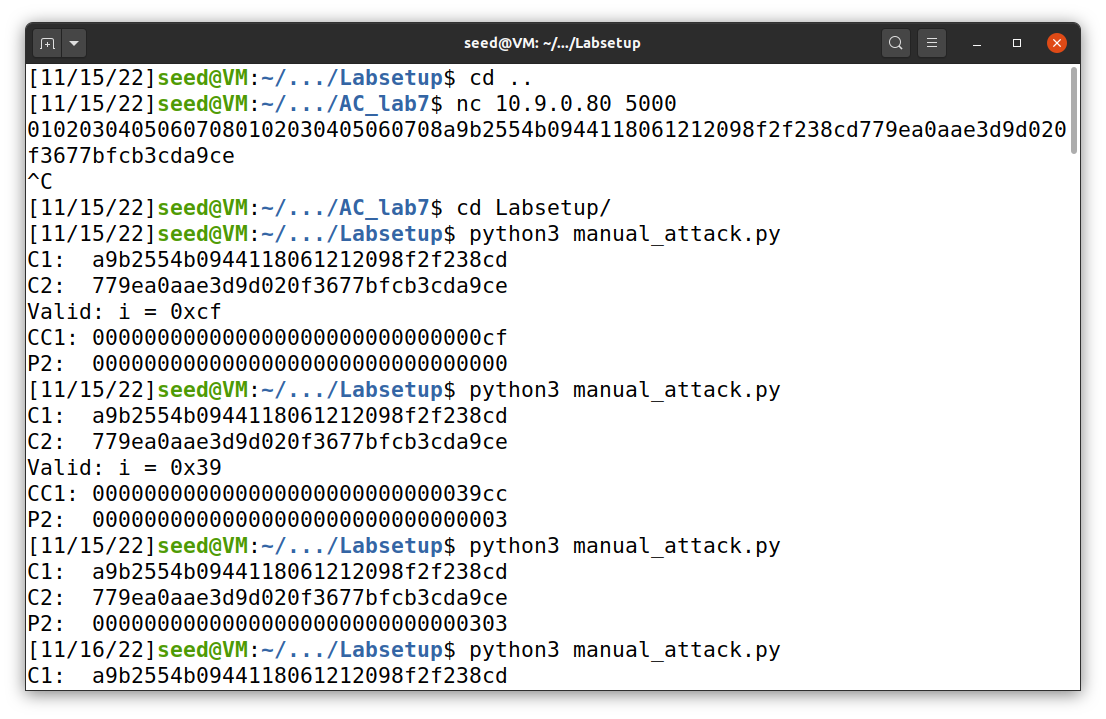


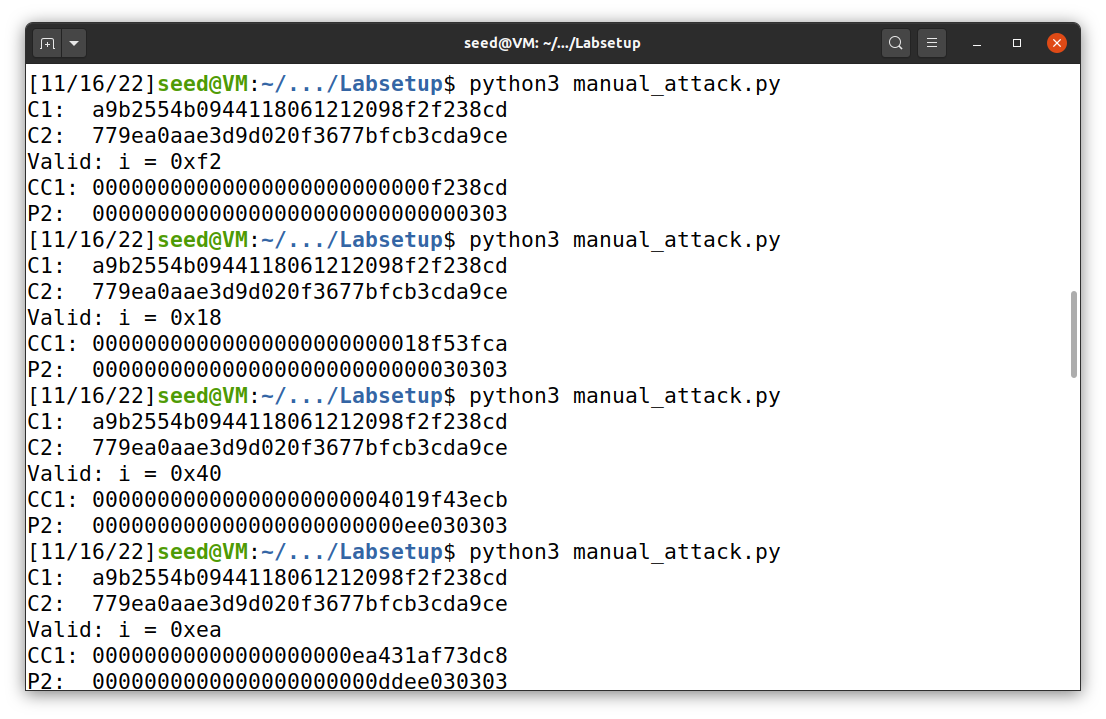
What do you deduce about the encryption scheme?

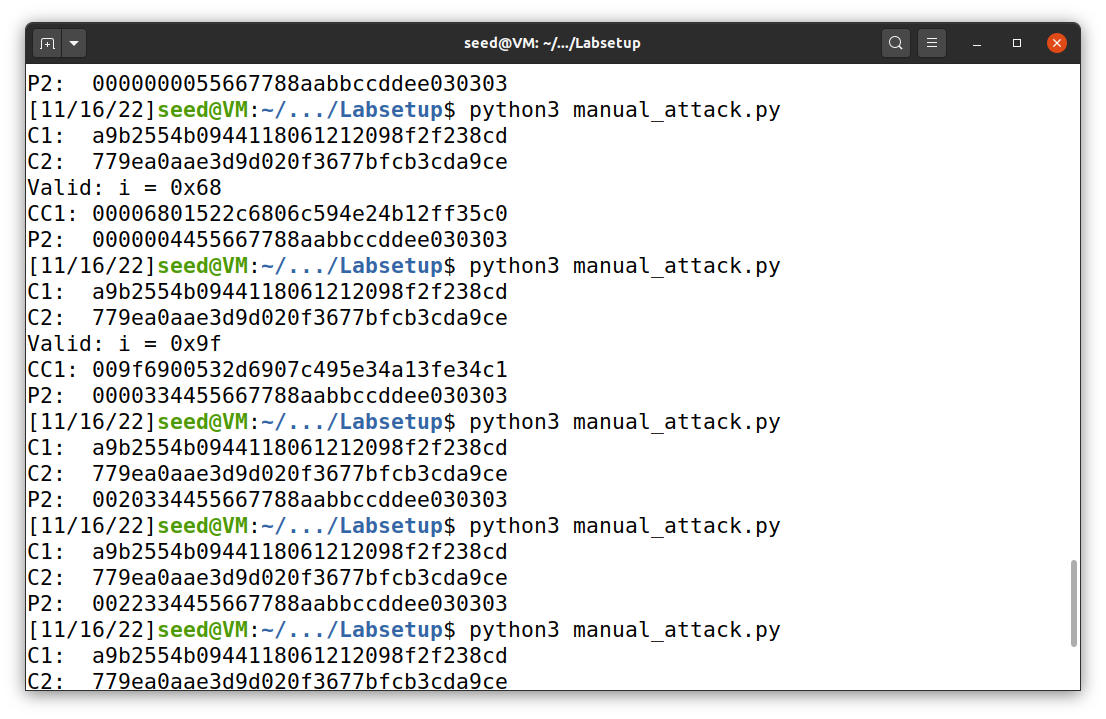
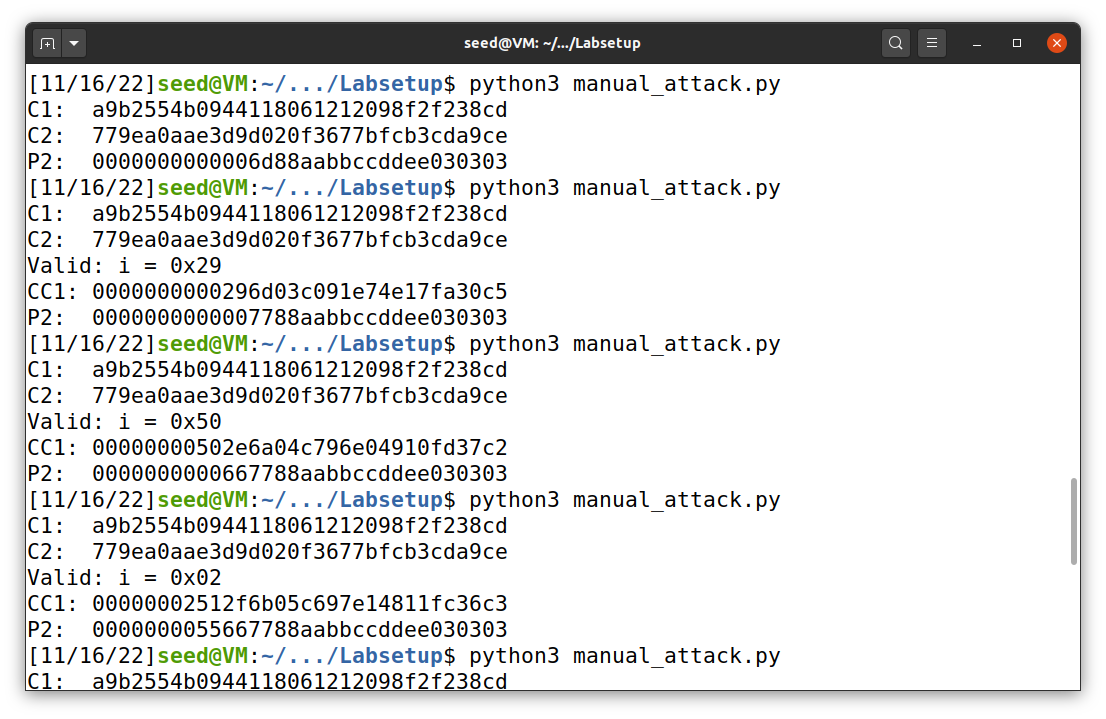
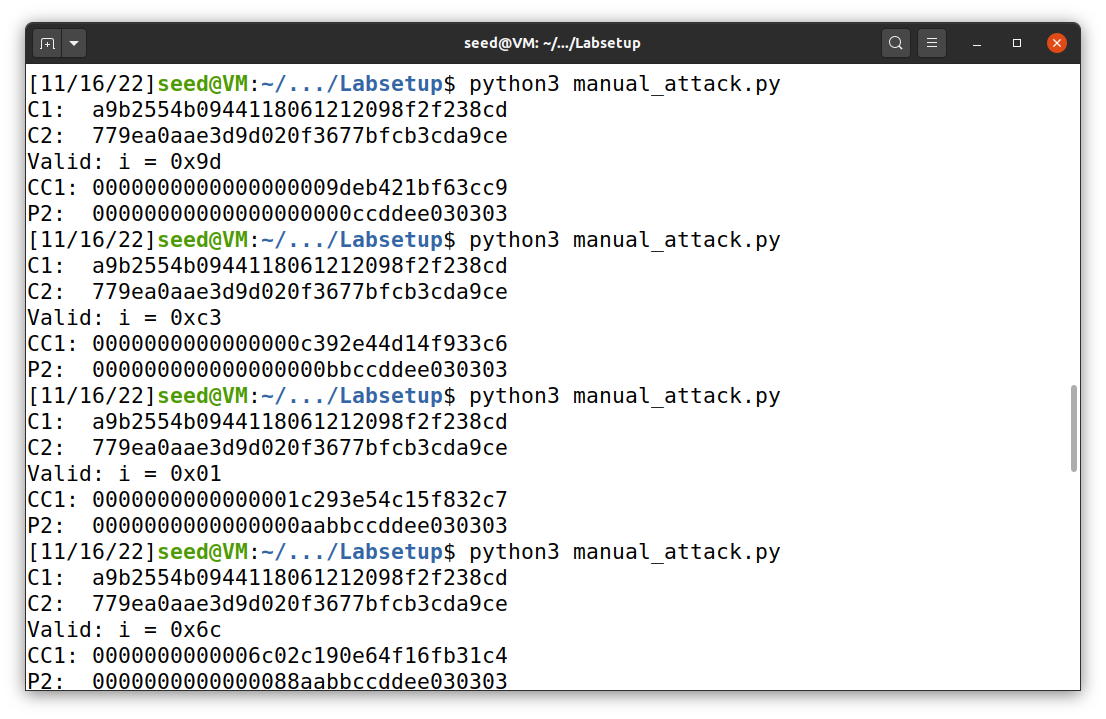
ANS: Padding is used to decrypt the ciphertext

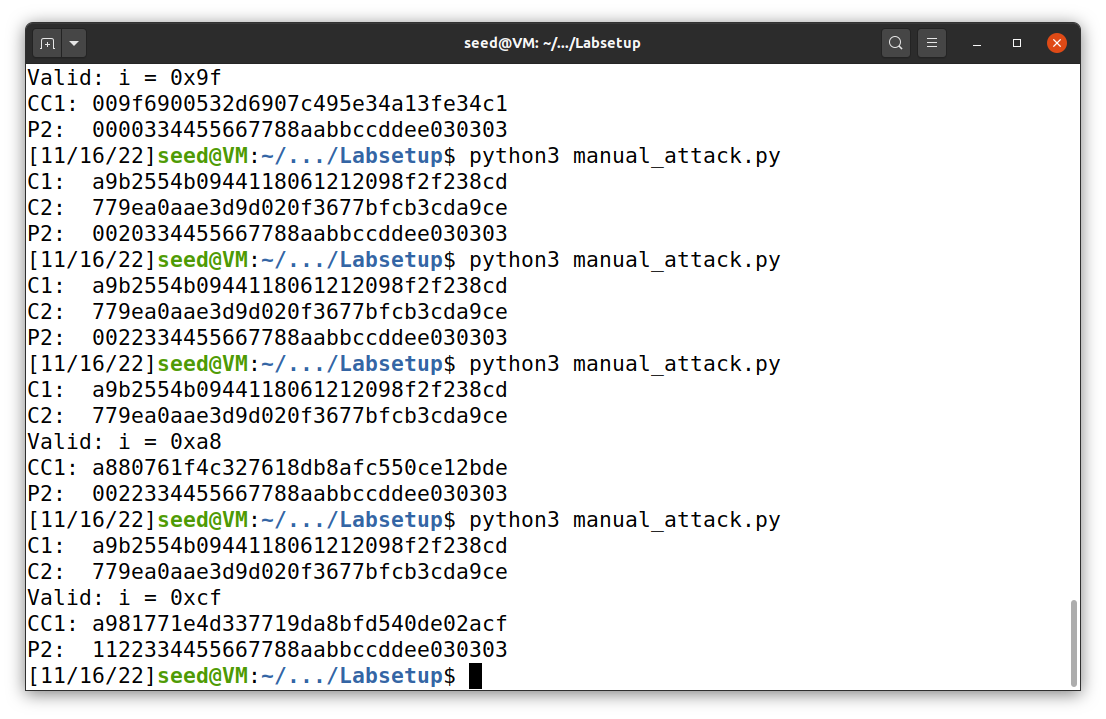
**Task 2: Padding Oracle Attack**

**Step 1 – Step 3 for 16 rounds**

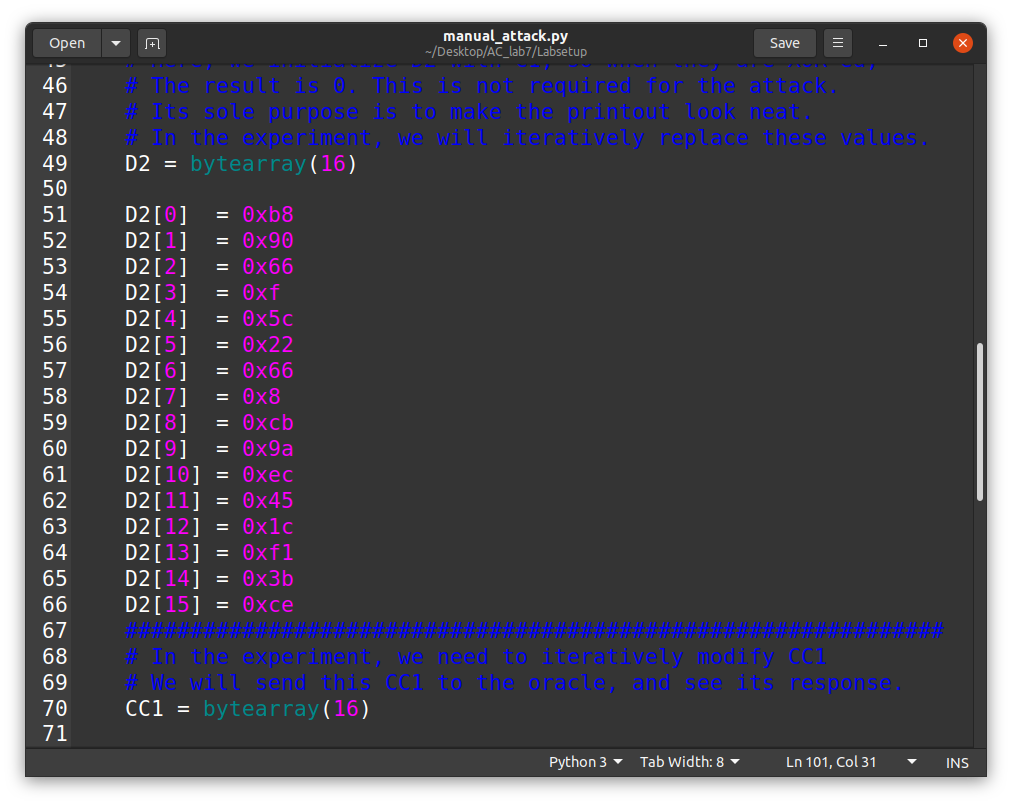


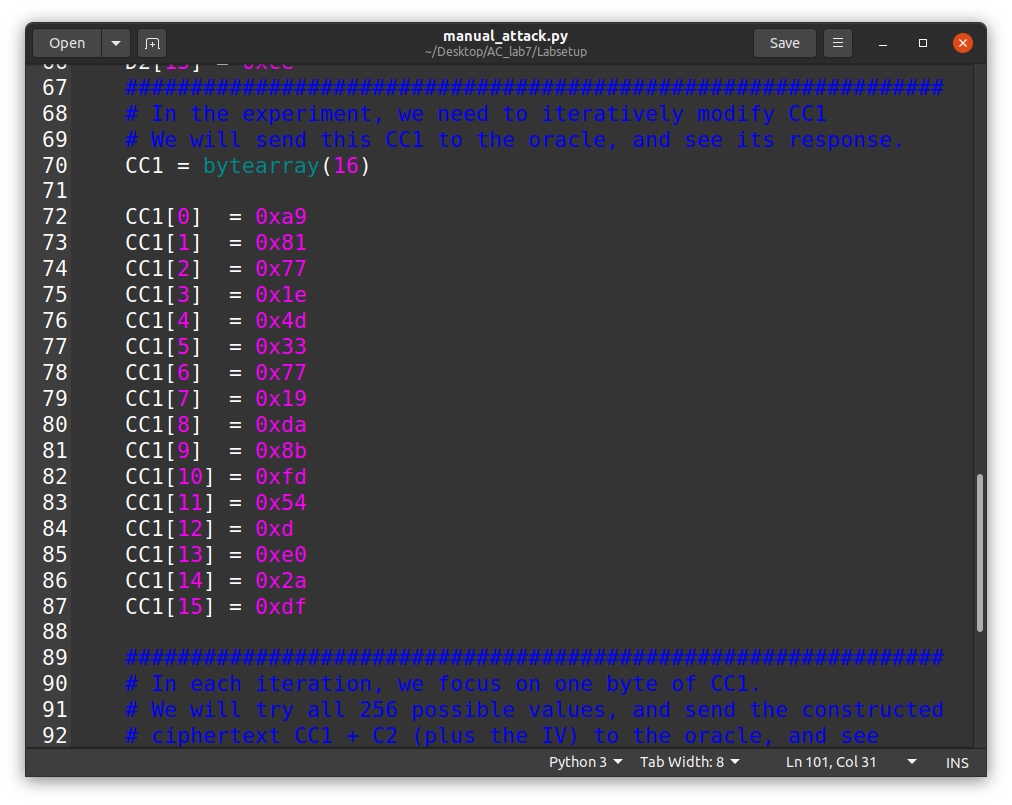






CODE:





**Task 3: Padding Oracle Attack(level 2)**

