

Applied Cryptography

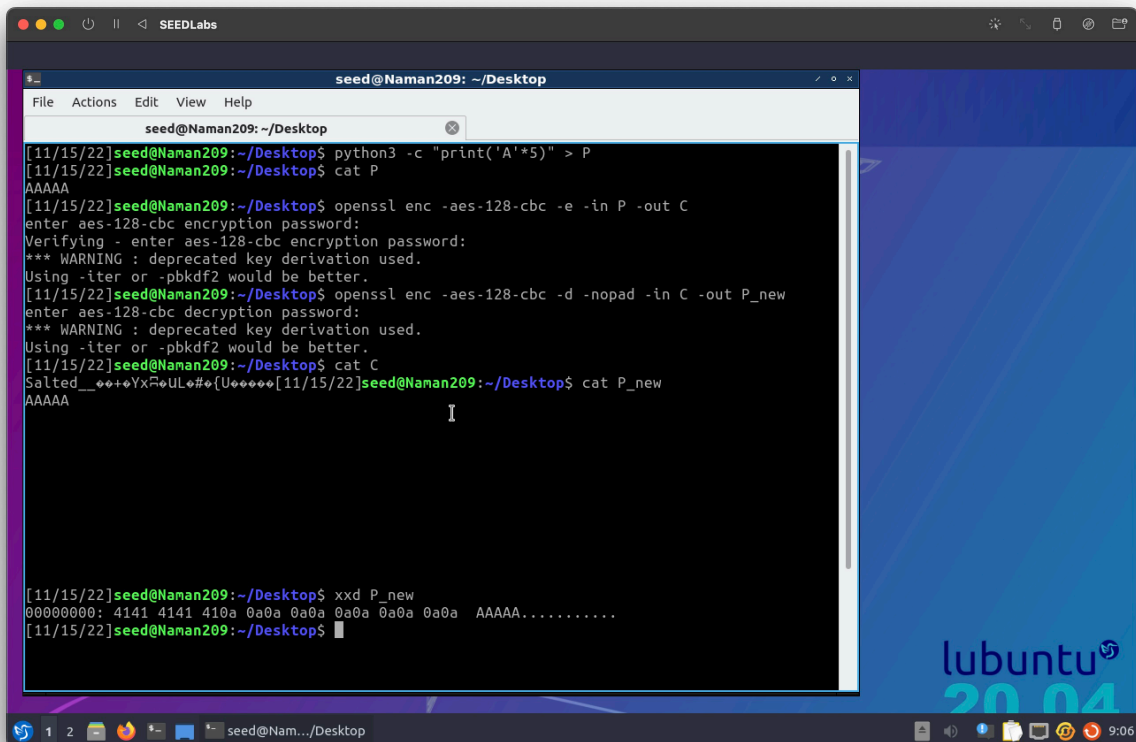
Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

Oracle Padding Attack

Task 1: Getting Familiar with Padding

```
$ python3 -c "print('A'*5)" >P
$ openssl enc -aes-128-cbc -e -in P -out C
$ openssl enc -aes-128-cbc -d -nopad -in C -out P_new
$ xxd P_new
```

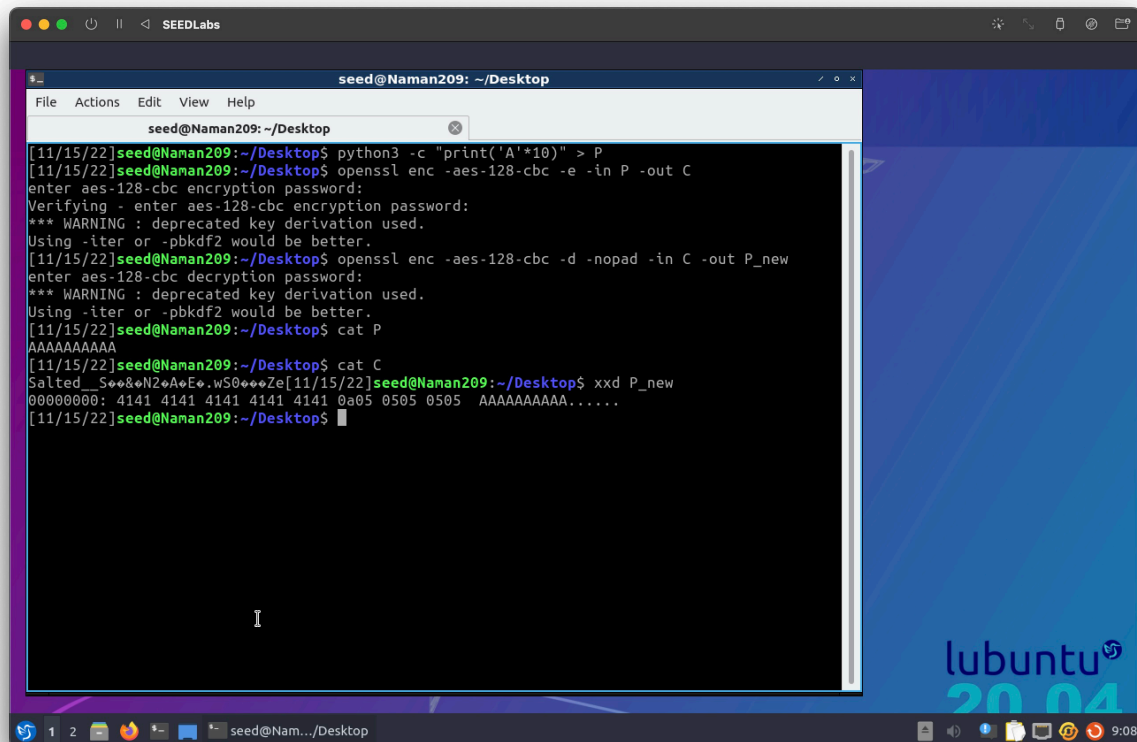
Bash



```
seed@Naman209: ~/Desktop
File Actions Edit View Help
seed@Naman209: ~/Desktop
[11/15/22]seed@Naman209:~/Desktop$ python3 -c "print('A'*5)" > P
[11/15/22]seed@Naman209:~/Desktop$ cat P
AAAAA
[11/15/22]seed@Naman209:~/Desktop$ openssl enc -aes-128-cbc -e -in P -out C
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[11/15/22]seed@Naman209:~/Desktop$ openssl enc -aes-128-cbc -d -nopad -in C -out P_new
enter aes-128-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[11/15/22]seed@Naman209:~/Desktop$ cat C
Salted__+++++YxRUL+{U++++[11/15/22]seed@Naman209:~/Desktop$ cat P_new
AAAAA
I
[11/15/22]seed@Naman209:~/Desktop$ xxd P_new
00000000: 4141 4141 410a 0a0a 0a0a 0a0a 0a0a 0a0a  AAAAAA.....
[11/15/22]seed@Naman209:~/Desktop$
```

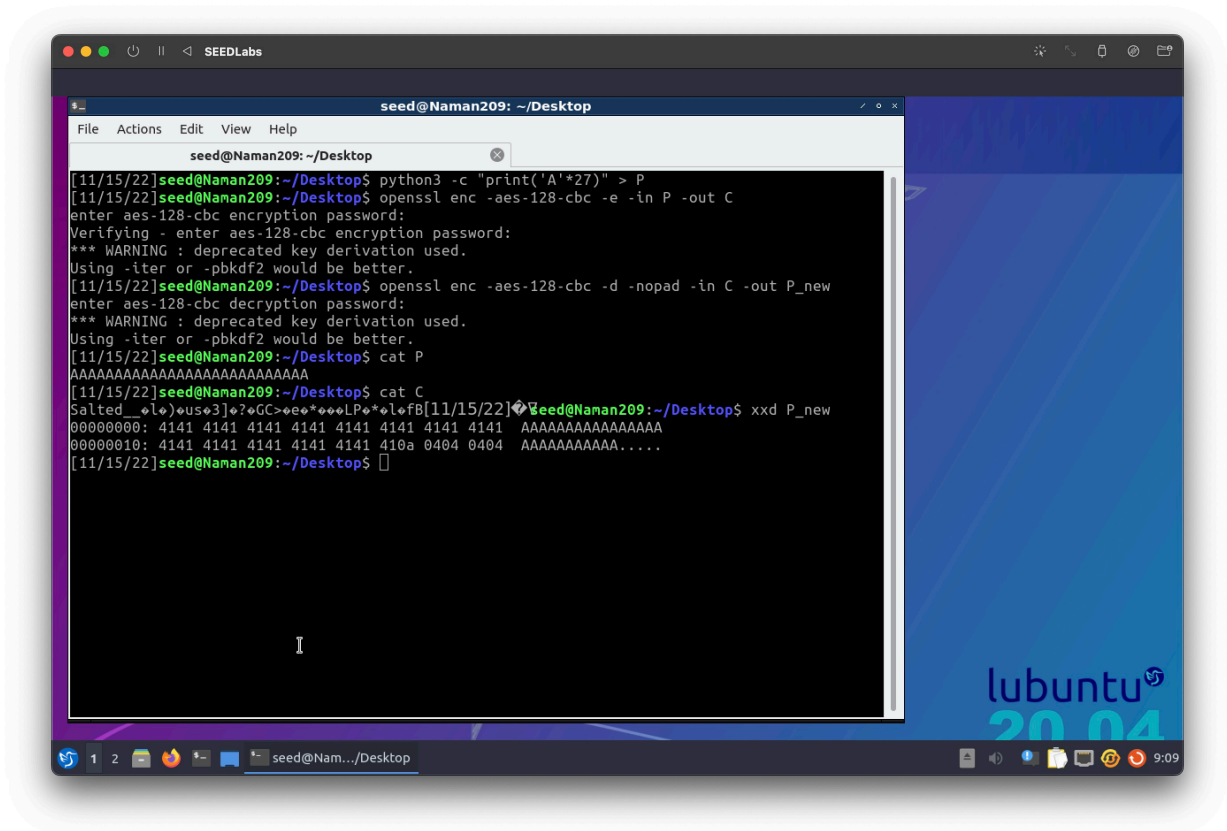
Bash

```
$ python3 -c "print('A'*10)" >P
$ openssl enc -aes-128-cbc -e -in P -out C
$ openssl enc -aes-128-cbc -d -nopad -in C -out P_new
$ xxd P_new
```



Bash

```
$ python3 -c "print('A'*27)" >P
$ openssl enc -aes-128-cbc -e -in P -out C
$ openssl enc -aes-128-cbc -d -nopad -in C -out P_new
$ xxd P_new
```



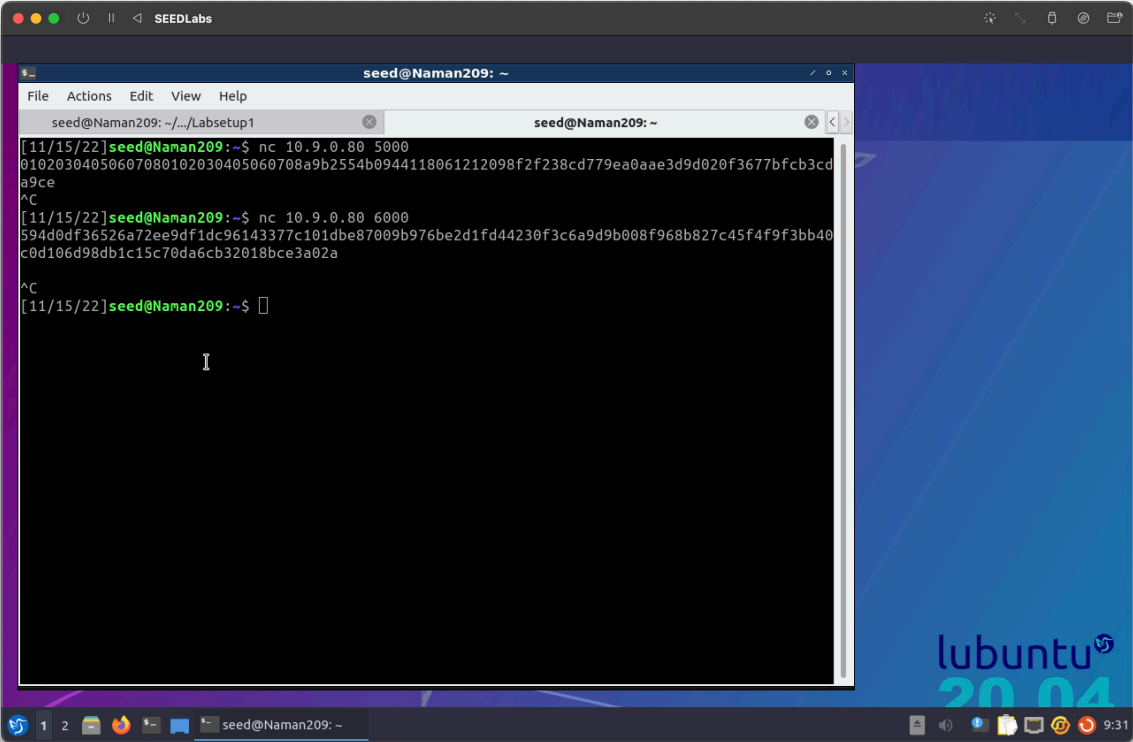
Question: What do you deduce about the encryption scheme?

Answer: The encryption scheme uses CBC mode and its security is proportional to input length

Task 2:Padding Oracle Attack (Level 1)

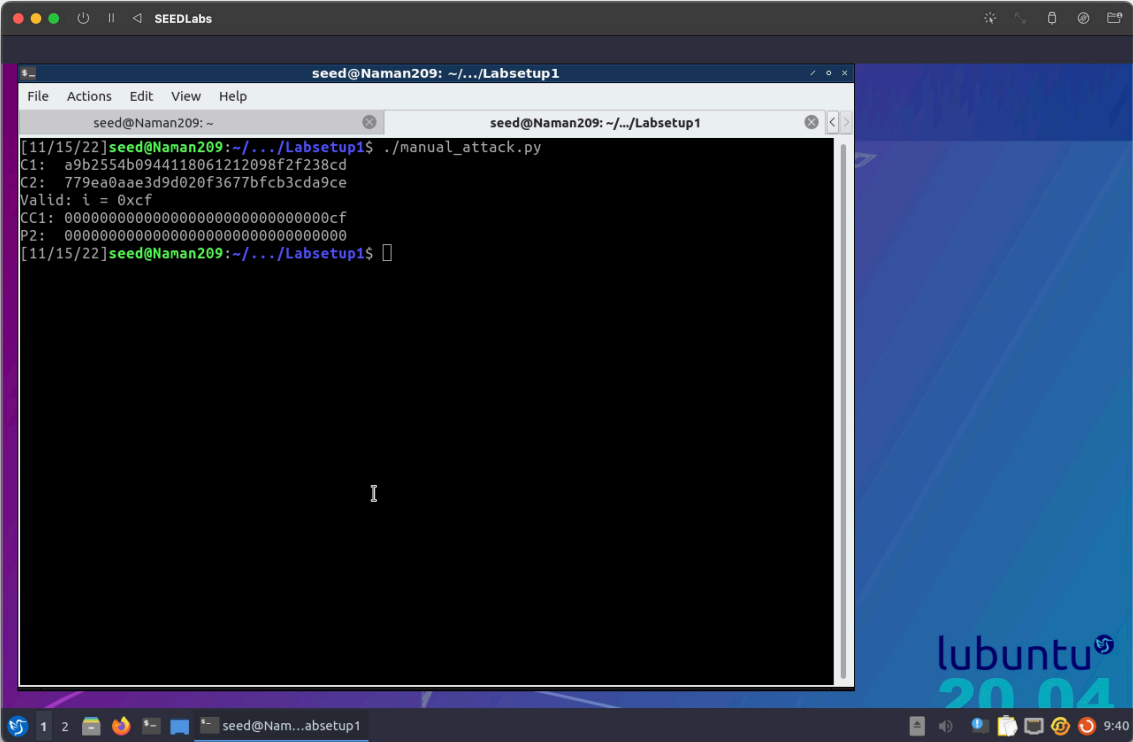
```
$ nc 10.9.0.80 5000 #level1  
$ nc 10.9.0.80 6000 #level2
```

Bash



```
$ ./manual_attack
```

Bash



```
>>> 0xcf ^ 2
205
>>> 0xcf ^ 1
206
>>> hex(206)
'0xce'
>>> hex(0xcf^0x2)
'0xcd'
>>> hex(0xcd^0x2)
'0xcf'
>>> hex(0xcd^0x1)
'0xcc'
>>> hex(0xcd^0x3)
'0xce'
>>> 
```

```
[11/15/22] seed@Naman209:~/.../Labsetup1$ ./manual_attack.py
C1: a9b2554b0944118061212098f2f238cd
C2: 779ea0aae3d9d020f3677bfc3cda9ce
Valid: i = 0xcf
CC1: 000000000000000000000000000000cf
P2: 00000000000000000000000000000000
```

```
[11/16/22]seed@Naman209:~/.../Labsetup1$ python3 manual_attack.py
Valid: i = 0xb7
CC1: b7
Valid: i=0xb775f0ac2783a012e7f889f03ab2d10e
P2: 1122334455667788aabbccdde030303
[11/16/22]seed@Naman209:~/.../Labsetup1$
```

Task 3:Padding Oracle Attack (Level 2)

```
$ ./automated_attack
```

Bash

```
[11/16/22]seed@Naman209:~/.../Labsetup1$ ./automated_attack.py
C1: ae7e345e56ffd42caa0416242cb3b2dc
C2: 666960ef493112c7a2ee1c1290e18ce7
Valid: i = 0xb8
CC1: 00000000000000000000000000000000b8
P2: 00000000000000000000000000000000
```