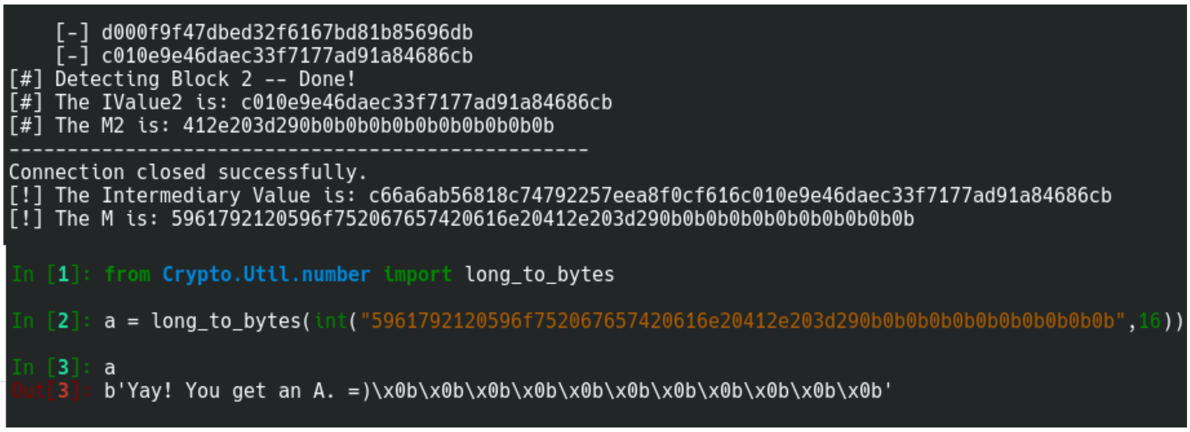

```
    [-] d000f9f47dbed32f6167bd81b85696db
    [-] c010e9e46daec33f7177ad91a84686cb
[#] Detecting Block 2 -- Done!
[#] The IValue2 is: c010e9e46daec33f7177ad91a84686cb
[#] The M2 is: 412e203d290b0b0b0b0b0b0b0b0b0b0b
--------------------------------------------------
Connection closed successfully.
[!] The Intermediary Value is: c66a6ab56818c74792257eea8f0cf616c010e9e46daec33f7177ad91a84686cb
[!] The M is: 5961792120596f752067657420616e20412e203d290b0b0b0b0b0b0b0b0b0b0b

In [1]: from Crypto.Util.number import long_to_bytes

In [2]: a = long_to_bytes(int("5961792120596f752067657420616e20412e203d290b0b0b0b0b0b0b0b0b0b0b",16))

In [3]: a
Out[3]: b'Yay! You get an A. =)\x0b\x0b\x0b\x0b\x0b\x0b\x0b\x0b\x0b\x0b\x0b'
```

```python
from oracle import *
from Crypto.Util import strxor
import re

C = '9F0B13944841A832B2421B9EAF6D9836813EC9D944A5C8347A7CA69AA34D8DC0DF70E343C4000A2AE35874CE75E64C31'
BLOCK = 2
C = re.findall('.{' + str(len(C) // (BLOCK + 1)) + '}', C)

Oracle_Connect()
M = []
IVALUE = []
for b in range(BLOCK):
    print('[*] Detecting Block', b+1)
    IV = C[b]
    Ivalue = []
    iv = '00000000000000000000000000000000'
    iv = re.findall('.{2}', iv)[::-1]
    padding = 1

    for l in range(16):
        print("  [+] Detecting IVALUE's last", l + 1 , 'block')
        for ll in range(l):
            iv[ll] = hex(int(Ivalue[ll], 16) ^ padding)[2:].zfill(2) #更新 iv

        for n in range(256):
            iv[l] = hex(n)[2:].zfill(2)
            data = ''.join(iv[::-1]) + C[b + 1]
            ctext = [(int(data[i:i + 2], 16)) for i in range(0, len(data), 2)]
            while True:
                try:
                    rc = Oracle_Send(ctext, 2)
                    break
                except:
                    print("reconnect")
                    Oracle_Connect()

            print("*")
            if rc != 48:
                Ivalue += [hex(n ^ padding)[2:].zfill(2)]
                break

        print('\n    [-]', ''.join(iv[::-1]))
        print('    [-]', ''.join(Ivalue[::-1]))

        padding += 1

    Ivalue = ''.join(Ivalue[::-1])
    IVALUE += [Ivalue]

    m = re.findall('[0-9a-f]+', str(hex(int(IV, 16) ^ int(''.join(Ivalue), 16))))[1]
    M += [m]

    print('[#] Detecting Block', b + 1 ,'-- Done!')
    print('[#]', 'The IValue' + str(b + 1), 'is:', Ivalue)
    print('[#]', 'The M' + str(b + 1) , 'is:', m)
    print('-' * 50)

Oracle_Disconnect()

print('[!] The Intermediary Value is:', ''.join(IVALUE))
print('[!] The M is:', ''.join(M))

```