Özge Öneyman 24906

Homework 4

Question 1

After using RSA_Oracle_Get() function, to find c_ I used this ((pow(2, e, N) * c) % N) equation. As a result of this,
m equals to :

```
Bravo! You find it. Your secret code is 3777
```

Question2

10000 possible combination for plaintext. The range of R is 128 to 255. With using these informations and RSA_OAEP_Enc() function I found the values in below:

```
print(PIN_)  ## The randomly choosen PIN is 1832.
print(R)     ## R is equal to 254.
```

Question3

To finding the message I used pow and modinv functions and as a result of this I found the below message:

```
### The message is: I am gonna make him an offer he cannot refuse
```

Question4

I can recover m2 using the given settings, because r1 and r2 are same.

```
print(message2)    ##The message 2 is Well, it was more like a command, no was not
an option!
```

Question5

To finding the private key I used pow and modinv functions and as a result of this I found the below key:

```
## The private key is
180114935909579198431966542725302564519161305719138984175086511374 37
```

Question6

To finding the private key I used pow and modinv functions and as a result of this I found the below key:

```
## The private key is: 665686245000902351298905661303992112436332170l4
```