Homework #4

1.

Let r be a random integer.

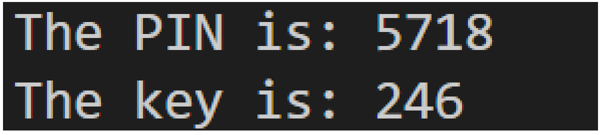
And give this to the query:
Q = (C * (r^e mod(N))
When we give it to the server, it returns us:
Q^d mod N = (C^d * (r^{ed} mod(N))mod(N) = C^d *r^{ed} mod(N)
We also know that C = m^e
Then,
C^d *r^{ed} mod(N) = m^{ed} * r^{ed} mod(N)
By theorem, we know that e * d = 1 mod(phi(N)), which means if they are in exponent, the exponent will be equal to 1.
Then, the server returns us:
ans= m*r mod(N)
m = r^{-1} * ans mod(N)
When we do such steps, I got:
Bravo! You found it. Your secret code is 25667, and when I send it to server, I got:
Congrats

2.

I selected a random four-decimal digit PIN and encrypted it using RSA. Your mission is to find the randomly chosen PIN.

By implementation, we know that random key is between [2^7 and 2^8 -1], which is not a huge set (given in code). We also know that pin is between [1000,10000). Then for every random key, we can try every possible pin and see if it is equal to ciphertext.

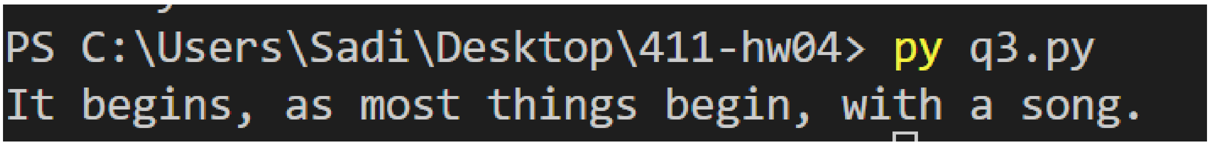
When we try every pin for every random key value and encrypt it with RSA_OAEP_Enc Function, we will get an encrypted value. If we compare it with our c and find an equal one, we will get the answer:



```
The PIN is: 5718
The key is: 246
```

3. The flaw is k = random.randint(1, 2**16-1). Which means our random key is between 1 and 2^{16}-1. Then, for every random key we can try to do ElGamal. By definition of ElGamal:

r = g^k modp
Then we will look for every possibility of random k that makes it equal with r.
When we find such k, we know the formula:
M = g^{-k} * t mod(p)
By theorems of modulus arithmetic:
M= g^{-k} mod(p) *t mod(p)
When we code the logic above, we get the answer:



```
PS C:\Users\Sadi\Desktop\411-hw04> py q3.py
It begins, as most things begin, with a song.
```

4. We see that r1 = r2

Then they may have same k value. Assuming that they have the same k value, they would have the same B^k value. First, we should calculate B^k:

$B^k = m^{-1} * t1 \bmod(p)$ since $t = B^k * m \bmod(p)$

We know that

$T2 = B^k * m2 \bmod(p)$

Then $m2^{-1} = B^k * t2^{-1} \bmod(p)$

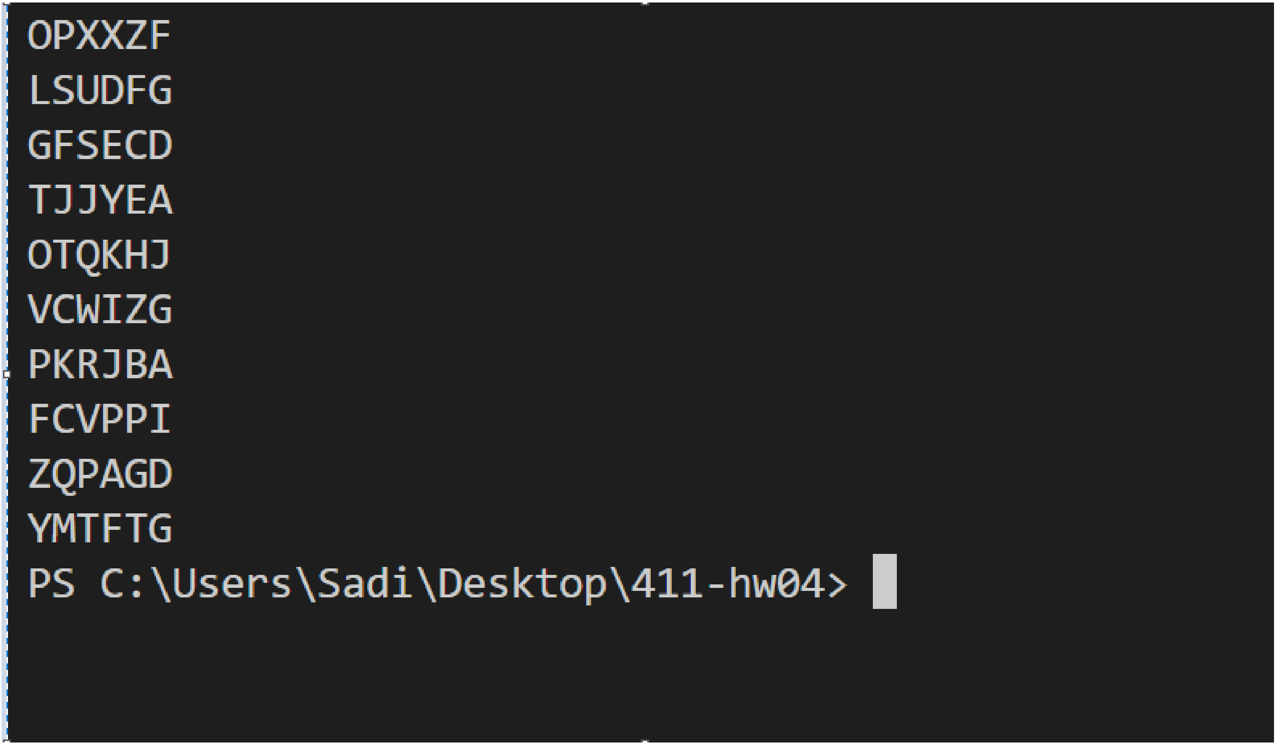
With this way, we can find m2: b'In sorrow, seek happiness.'

5.

First, thing we need to do is to find which last columns works for us. For every digest, we reduct and see if the reduction is in last columns array. If not, we hash the reducted version and do all over the process again until we find such value that is in last columns array ((t-2) * i trials).

Then, we found our row which gives us an initial value. Via hashing and reduction until we find our digest, we can find the passwords, which gives the answer. (Comparing hashes with our digests).

Here is the screenshot of answers (from digest 0 to digest 10):



```
OPXXZF
LSUDFG
GFSECD
TJJYEA
OTQKHJ
VCWIZG
PKRJBA
FCVPPI
ZQPAGD
YMTFTG
PS C:\Users\Sadi\Desktop\411-hw04>
```