CIS 4930 - 002: Fall 2018
Homework - 2

Total Points: 100
Due: Friday 10/12/2018

1 Objective

The objective for this assignment is to make sure

- You are familiar with native Python and Python syntax.
- You can write small programs that demonstrate Python's capabilities.
- You can use Python to solve small problems.
- You are comfortable with Python's Object Oriented Programming concepts.
- You can do some research on a particular problem and learn about its general background and then use Python to solve the problem. You will be expected to do this at any Software Engineering job, and it is good to practice while you're still in school.

2 RSA

The RivestShamirAdleman system is a simple public key cryptosystem that is based on prime numbers. Here's a very basic outline of how to encrypt using RSA

1. Generate 2 prime numbers `p` and `q`. `N = p*q`. `N` is the modulus.
2. The Totient Function λ(N) = (p-1)*(q-1).
3. Choose an integer `e` such that 1<e <$\lambda(N)$ and GCD(e,$\lambda(N)$) = 1.
4. Choose an integer `d` such that `e * d mod` λ`(N) = 1`. You need to use the Extended Euclid Algorithm to determine `d`
5. Now, you can encrypt a message by using c = m^e mod N
6. You can decrypt the ciphertext, using m = c^d mod N

You can find more information of RSA here: `https://en.wikipedia.org/wiki/RSA_(cryptosystem)`

3 Specifications

For this homework, you will write a program that involve Python concepts like classes, decorators, generators and iterators. You will be writing an RSA encryption/decryption system that conforms to the following specifications.

- Write a class called `RSA` that will contain all of the functions in the program. In the constructor for `RSA` initialize an empty list and set variables `e` and `d` to 0. (10 points)
- Write a function called `inputFunc` that reads in the number of entries from the user. Then, read in those many values and add them to the list. (5 points)

- Write a function called `printFunc` that takes in a number and prints "message is " followed by the number. (5 points)
- Write a generator function called `primeGen` that will take a minimum value as a parameter and then yield the next prime numbers. Please note that this input parameter will be quite large and you might want to use `long` if you're using Python 2. (10 points)
- Write a function called `keyGen`. This function will read in a minimum value from the user. Then, it will use the `primeGen` generator to get the next 2 prime numbers and generate the value `N` and the keys `e` and `d`. Print `e` and `N` but not the other values. (10 points)
- You would probably also need to write helper functions for the Lowest Common Multiple (LCM), Greatest Common Divisor (GCD) and the Totient function.
- Write a function called `encrypt` that takes in a number as a parameter and returns the RSA encrypted value of the number. (5 points)
- Write a function called `decrypt` that takes in an encrypted number as a parameter and returns the RSA decrypted value. (5 points)
- Write a decorator function for `printFunc` that will print "The encrypted " before the printed message. (10 points)
- Write another decorator function for `printFunc` that will print "The decrypted " before the printed message. (10 points)
- Write a function called `messages` that calls `inputFunc` and `keyGen` and then, uses an iterator to iterate through the list and encrypts each of the numbers using the `encrypt` function. Store the results in another list. Then, go through the second list and print each encrypted number using the decorator for the encrypted message. (15 points)
- Verify your results be decrypting each of the encrypted messages and checking if you get the old value back. Print the decrypted values using the decorator for the decrypted message. (10 points)
- In main, create an RSA object and call the `messages` function. (5 points)

4 Sample Output

This section shows the sample output for the program. Please note that the exceptions raised when the iterator hits the end of the list is not included here, since I checked for the exception while generating the output. Please make sure you do so as well. Also, you might have different values even if you have the same inputs, depending on how 'e' is chosen. As long your decrypted message matched your initial input, you should be fine.

```
Enter the number of messages: 5
Enter the messages:
15
97
201
49
500
Enter the minimum value for the prime numbers: 20304
N is 413105621
e is 286049
The encrypted message is 106412658
The encrypted message is 367869867
```

```
The encrypted message is 393299060
The encrypted message is 70473606
The encrypted message is 409030235
The decrypted message is 15
The decrypted message is 97
The decrypted message is 201
The decrypted message is 49
The decrypted message is 500
```

5 Submission

- Try and use Python 3 as much as possible. For this homework, version should just affect the print function and the size of the integer type.
- Please name your file `RSA.py`
- Please add your name and FSUID as a comment at the top of your programs.
- We are aware that Python has libraries that would let you one line these problems. However, we are just testing your understanding of Python Object Oriented Concepts. Please try and write Pythonic code (exploit the features of Python to try and write as few lines as possible).
- Please turn in the program through Canvas.
- We are also aware that solutions to these problems exist on the internet. Please turn in your solution to the problem, and not someone else's. We will be running your submission through plagiarism detection software.
- You are also responsible for making sure your submission on Canvas contains the right file and that the file has not been corrupted in any way.