Task 6

The decrypted message is:
https://en.wikipedia.org/wiki/RSA_(cryptosystem)#Attacks_against_plain_RSA

How I approached the problem:
I tried to understand the rsa.py file we were given. Based on my knowledge about RSA and key pairs I knew that all I had to do was to find the private key, as this and the encrypted message (as we had) were the two arguments used for decrypting. When I looked at the code, I saw that the public key was on the form (e, n) and that n=p*q, in which have to be known for finding the private key. Therefore, I found two primes if multiplied equals 100127, in which was 223 and 449. Then I rewrote the methods from Donn and made the program decrypt it for me with the new private key.

What are the problems with this simple implementation of RSA, and how can you solve it?
Well, one of the main problems I see is that given that you have the public key, it is possible to find the secret key if you know which algorithm is used for generating the key pairs. One of the solutions is the one implemented in networking called three-way-handshake. In this protocol each side generate its own secret after telling each other which algorithms can be used by both sides. Then they work together in finding a keypair based on the first one creating a secret, the second one trying to solve it and as both of them has created the keypair and confirmed it without actually giving away the public key - it is a little bit safer.

Secondly is the fact that it is possible to crack the code with a machine checking millions of combinations in a short amount of time. As a result of this, prime numbers is used in cryptography as primes are harder to work with mathematically. Here is where the P=NP problem come in. As the security of modern cryptography is based singlehandedly on insanely large prime numbers (as these are harder to calculate), if you find a way to quickly solve every problem that is quickly verified, you have access to basically all the information in the whole society by now. If you can solve equations with huge prime numbers within seconds or even days, cryptography is not even a thing anymore. The solution on this is to hope that NP not equals P, and to find even larger prime numbers.