Problem 8.1

a) Given public key, $k = (e, n)$ and ciphertext c. To ~~crack~~ eavesdrop RSA, we need to get p & q whose multiplication, N, we have.

Inserting N in Prime Factor generator gives us p and q. It's only possible since the number is not massively large.

With that we calculate $\phi(N) = (p-1)(q-1)$

And to get d, for decrypting (d, n) we compute as follow:

$$ed \bmod \phi(N) = 1$$

$$ed = 1 \bmod \phi(N)$$

We put this equation in a python file to generate d more efficiently. The code is attached in the homework.

b) Runing the code yields ~~the following result:~~ is a list of character code points. When converted to Unicode it says:
This is not really a secret.

Problem 8.2

A	Public	B
$a = 112$	$p = 181$	$b = ?$
	$g = 24$	

a) Alice sends $g^a \bmod p = 24^{112} \bmod 181$

$= 126$

b) $k = 27$,