Problem Sheet 6

Problem 6.1

Solution:

b)
We have public key e = 15852553, n = 44331583. Now we need to find $\Phi(n)$:
$\Phi(n) = (p-1)(q-1)$
$n = pq$
Find all possible unique combinations of pq, and calculate $\Phi(n)$ for them. To do that in the most efficient ways, iterate from 0 to square root of n (i for counting), and divide n by i, if no reminder, then they are possible pq.
Next, we need to find d, iterate through all $\Phi(n)$, and for each iterate from 0 to $\Phi(n)_i$. If $edmod\Phi(n) = 1$, save d as possible key. Now, try decoding them.
Since, we know that our text is ascii text, values should be in range 0-255. If all decoded values are in that range, we found key (most probably). b)
Go, go away corona virus!

Problem 6.2

Solution:

F80EC110C068139E49AF66FF9CE45948346EEE2CD8C7D1908ACE8D0A00005591