5) Consider the RSA scheme with public key $(e, n) = (23, 407)$.

Using this scheme, encrypt the message $M = 321$.

To encrypt this message, we compute M^e and reduce modulo n to a value between 1 and n.

$$C \equiv M^e \equiv 321^{23} \pmod{407}$$

This value is difficult to compute without a calculator. However we can try some sort of splitting the modulus technique. Notice that $407 = 11 \cdot 37$. Thus, it suffices to compute (we used the fact that $30 \cdot 11 = 330$ so $321 \equiv 2 \pmod{11}$)

$$C \equiv 321^{23} \equiv 2^{23} \equiv (2^{10})^2 2^3 \equiv (1)8 \equiv 8 \equiv 30 \pmod{11} \qquad \text{By FLT}$$

and (using that $37 \cdot 3 = 111$ and $37 \cdot 4 = 148$ and $37 \cdot 5 = 185$)

$$\begin{aligned} C &\equiv 321^{23} \equiv 25^{23} \equiv 5^{46} \equiv 5^{36} 5^{10} \equiv 5^{10} \pmod{37} \qquad \text{By FLT} \\ &\equiv 125^3 \cdot 5 \equiv 14^3 \cdot 5 \equiv 196 \cdot 14 \cdot 5 \pmod{37} \\ &\equiv 11 \cdot 70 \equiv 11 \cdot (-4) \equiv -44 \equiv 30 \pmod{37} \end{aligned}$$

Now, combining using CRT shows that $C \equiv 30 \pmod{407}$ and hence that $C = 30$.

Determine the private key corresponding to the public key $(23, 407)$.

Above, we shows that $407 = 11 \cdot 37$ and hence $\phi(n) = (p-1)(q-1) = 10 \cdot 36 \equiv 360$. Thus, we are trying to solve $ed \equiv 1 \pmod{\phi(n)}$ or in other words

$$23d \equiv 1 \pmod{360}$$

This is equivalent to

$$23d + 360k = 1$$

for some integer k. We will solve this using EEA:

d	k	r	
0	1	360	
1	0	23	
-15	1	15	15
16	-1	8	1
-31	2	7	1
47	-3	1	1

Hence $23(47) + 360(-3) = 1$ and thus $d = 47$ is the inverse.