

Problem 3:

I found a broad variety of answers for problem 3. For part 1, I give credit for (good) intuition at the answer. However, some (not so good) intuition is not given any credit, such as making it hard to guess n ; n is part of the public key $\{e, n\}$ so it's already public.

The correct answer for part 2 should be $p=19, q=2$, giving $n=38$. Then, public and private key pairs may be $\{5, 38\}$ and $\{11, 38\}$; note that $55 \bmod 18 = 1$.

e.g.

$$\begin{aligned} m=2: \quad 2^5 \bmod 38 &= 32 && (=c) \\ c=32: \quad 32^{11} \bmod 38 &= 2 && (=m) \end{aligned}$$

However, I also allow the following answers although they are not workable in practice.

1. Choosing $n=28$, which means you have $p=7, q=4$. Obviously, q is not a prime. As a result, it does not encrypt anything.

$$\begin{aligned} m=7 \quad 7^5 \bmod 28 &= 7 \\ c=7 \quad 7^{11} \bmod 28 &= 7 \end{aligned}$$

2. Choosing $e=1$ and $d=19$. Although $19 \bmod 18 = 1$, using 1 as key doesn't encrypt anything when $m < n$.

$$m=5 \quad 5^1 \bmod 38 = 5$$
