Problem 0.1 (Chapter 15, problem 1)**.** Find the primes p, q, given that $pq = 18779$ and $(p-1)(q-1) = 18480$.

Proof. We know that

$$p + q = pq - (p-1)(q-1) + 1 = 18779 - 18480 + 1 = 300$$

We also know that

$$p - q = \sqrt{(p+q)^2 - 4pq} = \sqrt{14884} = 122$$

Therefore

$$p = \frac{1}{2}((p+q) + (p-q)) = 211$$

and

$$q = \frac{1}{2}((p+q) - (p-q)) = 89.$$

□

Problem 0.2 (Chapter 15, problem 2)**.** In this problem we will use the public key $(N, e) = (143, 11)$.

(a) Encode the message WHEREAREYOU.

(b) You intercept the message

$$12, 59, 14, 114, 59, 14$$

Decode this message.

Proof. For part (a), we first convert the message to numbers, getting

$$23, 8, 5, 18, 5, 1, 18, 5, 25, 15, 21$$

By the way, the book is a bit unclear about how exactly you are supposed to convert between letters and numbers. The above scheme seems like the simplest to me, and is consistent with part (b). But if you picked a different way, that is fine too. To encode these numbers, we raise them to the 11th power modulo 143. This gives

$$\begin{aligned}
23^{11} &\equiv 56 \pmod{143} \\
8^{11} &\equiv 96 \pmod{143} \\
5^{11} &\equiv 60 \pmod{143} \\
18^{11} &\equiv 73 \pmod{143} \\
1^{11} &\equiv 1 \pmod{143} \\
25^{11} &\equiv 25 \pmod{143} \\
15^{11} &\equiv 59 \pmod{143} \\
21^{11} &\equiv 109 \pmod{143}
\end{aligned}$$

(If you wanted to do these computations by hand, you could use repeated squaring. I used a computer). So, our encoded message is

$$56, 96, 60, 73, 60, 1, 73, 60, 25, 59, 109$$

For part (b), we crack the code by computing that $143 = 11 \cdot 13$. Thus, $p = 11$ and $q = 13$. Therefore $(p-1)(q-1) = 10 \cdot 12 = 120$. To find the decoding exponent d, we need to solve $11d \equiv 1 \pmod{120}$. In fact, $11^2 = 121$, so we can take $d = 11$. Now we compute

$$\begin{aligned}
12^{11} &\equiv 12 \pmod{143} \\
59^{11} &\equiv 15 \pmod{143} \\
14^{11} &\equiv 14 \pmod{143} \\
114^{11} &\equiv 4 \pmod{143}
\end{aligned}$$

So our decoded message is

$$12, 15, 14, 4, 15, 14$$

Converting this back to letters, we get

LONDON

□