Homework 26 Solutions

1. **Alice wishes to send a secret message to Bob using the public-key cryptographic protocol discussed in today's lecture (and in Chapter 22 of the book). Upon request, Bob sends her $n = 143$ and $k = 17$. If Alice wants to transmit the encrypted version of the message $m = 24$, what should she send Bob?**

   We encrypt messages by raising them to the k-th power $\pmod{n}$. In this case, that means that the encrypted message is $24^{17} \pmod{143}$. Successive squaring gives

$$\begin{aligned} 24^2 &\equiv 576 \equiv 4 \\ 24^4 &\equiv 16 \\ 24^8 &\equiv 256 \equiv 113 \equiv -30 \\ 24^{16} &\equiv 900 \equiv 42 \end{aligned}$$

   Thus $24^{17} \equiv 24^{16} \cdot 24 \equiv 1008 \equiv 7 \pmod{143}$. So Alice should send $\boxed{7}$ to Bob.

2. **Later, Ann wants to communicate with Bob. Bob chooses $p = 11$, $q = 17$, $k = 23$. After sending Ann $n = 187$ and $k = 23$, he receives from her the number 177. What was Ann's message?**

   To decode a message, we compute its k-th root $\pmod{n}$. In this case, this means we want to find $177^{1/23} \pmod{187}$. Fortunately, we're given that $187 = 11 \cdot 17$, and thus we can compute $\phi(187) = (11 - 1)(17 - 1) = 160$. We now need to solve $23x + 160y = 1$. The Euclidean algorithm gives

$$\begin{aligned} 160 &= 6 \cdot 23 + 22 \\ 23 &= 22 + 1. \end{aligned}$$

   Running it backwards gives

$$\begin{aligned} 1 &= 23 - 22 \\ 1 &= 23 - (160 - 6 \cdot 23) = -160 + 7 \cdot 23. \end{aligned}$$

   We conclude that $177^{1/23} \equiv 177^7 \pmod{187}$. Successive squaring gives

$$\begin{aligned} 177^2 &\equiv (-10)^2 \equiv 100 \pmod{187} \\ 177^4 &\equiv 10000 \equiv 98 \equiv -89 \pmod{187}. \end{aligned}$$

   Thus we have

$$177^7 \equiv 177^4 \cdot 177^2 \cdot 177 \equiv -89 \cdot 100 \cdot -10 \equiv 12 \pmod{187}.$$

   We conclude that Ann's message was $\boxed{12}$.