Homework 31 Solutions

1. **Alice and Bob decide to use the password protocol we discussed in class. They choose $p = 59$, and 2 as a multiplicative generator** $\pmod{59}$**. Alice chooses $k = 13$ as her secret exponent, and so she sends Bob $2^{13} = 50 \pmod{59}$. Bob chooses $m = 17$ as his secret exponent, and so he sends Alice $2^{17} = 33 \pmod{59}$. Now, what is their password?**

   Their password is $2^{17 \cdot 13} \pmod{59}$. Of course, neither one of them computes it in that way. Alice computes the password by doing $33^{13} \pmod{59}$, and Bob computes it by doing $50^{17} \pmod{59}$. These all give the same answer, although doing the computation the way Alice or Bob would is easier than computing $2^{17 \cdot 13} \pmod{59}$ directly. We will compute $33^{13} \pmod{59}$, since it has the smallest exponent. We have

   $$33^2 \equiv 1089 \equiv 27$$
   $$33^4 \equiv 729 \equiv 21$$
   $$33^8 \equiv 441 \equiv 28$$

   where all of these congruences are taken $\pmod{59}$. Thus we have

   $$33^{13} \equiv 33^8 \cdot 33^4 \cdot 33 \equiv 28 \cdot 21 \cdot 33 \equiv -2 \cdot 33 \equiv \boxed{52} \pmod{59}.$$

2. **Amanda is communicating with someone she hopes is Bob. For their digital signatures, Amanda and Bob have previously chosen $p = 31$ and 3 as a multiplicative generator** $\pmod{31}$ **(recall from the last homework that 3 is, in fact, a generator in arithmetic** $\pmod{31}$**). Amanda has 7 as her secret exponent, and thus has published 17, which is $3^7 \pmod{31}$, as the pubic part of her signature. She also knows that Bob has previously published 4 as the public part of his signature. If Amanda now receives a message claiming to be from Bob with the signature 16, should she believe that it's actually from Bob or not?**

   Amanda needs to compute their password and see if it's 16 or not. She does this by computing $4^7 \pmod{31}$. We have

   $$4^2 \equiv 16 \equiv -15$$
   $$4^4 \equiv 225 \equiv 8$$

   where all of these congruences are taken $\pmod{31}$. Thus we have

   $$4^7 \equiv 4^4 \cdot 4^2 \cdot 4 \equiv 8 \cdot -15 \cdot 4 \equiv -15 \cdot 32 \equiv -15 \equiv 16 \pmod{31}.$$

   So their password is 16, and thus Amanda should believe that the message is from Bob.