1. In the RSA cryptosystem, $de \equiv 1 \pmod{(p-1)(q-1)}$. Thus, given p, q, and d or e, we can easily find the missing value. First, we calculate $(p-1)(q-1) = (19-1)(29-1) = 18 \times 28 = 504$. From here, we must simply calculate the modular inverse of $e = 17$ to find d. Because this is a lengthy process and we've been over it in class before (using the Extended Euclidean Algorithm), I won't elaborate on how it is found, but this inverse is 89.

2. (a) To uniquely specify 132 elements, we need at least 8 binary digits; $2^7 = 128$, $2^8 = 256$.

   (b)

   (c) $143 = 11 \times 13$, So p and q are 11 and 13. This means

   $$(p-1)(q-1) = 10 * 12 = 120$$

   $$ed \equiv 1 \pmod{120}$$
   $$d = e^{-1} \pmod{120}$$
   $$d = 11$$

   This can be confirmed: $11 \times 11 = 121 \equiv 1 \pmod{120}$.

   (d)

   $$\begin{aligned} c = M^e \pmod{120} &= 5^{11} \pmod{120} \\ &= (5^3)^3 \times 5^2 \pmod{120} \\ &= 5^3 \times 5^2 \pmod{120} \\ &= 5 \times 5^2 \pmod{120} \\ &= 5 \end{aligned}$$

   And if we decrypt it, we know we will get 5 again, since in this special case the decryption function is the same as the encryption function.

3. K, the common key calculated by Alex and Bob, is equal to $a^{xy} \pmod{p} = 7^{xy} \pmod{71}$. Because 7 is a primitive root for $\mathbb{Z}_{71}^*$ we have $7^{70} \equiv 1 \pmod{71}$. So the question is now asking for two factorisations of 70. Therefore, $(x, y) = (7, 10), (2, 35)$.

4. (a) 8 is the largest primitive root for $\mathbb{Z}_{11}^*$.

   (b) K is equal to $8^{xy} \pmod{11} = 8^{5\times3} \pmod{11} = 10$.