Exercises: Diffie Hellman

1. Try to calculate these congruences without a calculator:

   (a) Calculate the lowest positive value of $3^4 \mod 80$.

   (b) Use your answer to the above to show that $3^{316} \equiv 1 \mod 80$.

2. Show $4^{5n+1} \equiv 0 \mod 1024$, for all integers n;

3. Calculate $11^n \mod 101$ for $n = 2, 3, 4, 5, 10$.

4. We will use Diffie Hellman key exchange to create a shared key. Let generator $x = 11$, and modulus $q = 101$.

   (a) If Alice's secret integer is $a = 13$, calculate $x^a \mod q$.

   (b) If Bob's secret integer is $b = 20$, calculate $x^b \mod q$.

   (c) Finally, calculate the shared secret $x^{ab} \mod q$.

   (d) Why can't we use $x = 10$ as our generator?