Exercises: Diffie Hellman

1. Try to calculate these congruences without a calculator:

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

   $$3^4 = 81 \equiv 1 \mod 80.$$

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

   $$3^{316} = (3^4)^{79} \equiv 1^{79} \equiv 1 \mod 80.$$

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

   By observation, $4^5 = 1024 \equiv 0 \mod 1024$. Hence,

   $$4^{5n+1} = (4^5)^n \times 4 \equiv 0^n \times 4 \equiv 0 \mod 1024, \text{ for all } n.$$

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

   $11^2 = 121 \equiv 20 \mod 101$

   $11^3 \equiv 11^2 \times 11 \equiv 20 \times 11 \equiv 220 \equiv 18 \mod 101$

   $11^4 \equiv (11^2)^2 \equiv 20^2 \equiv 400 \equiv 97 \mod 101$

   $11^5 \equiv 11^2 \times 11^3 \equiv 20 \times 18 \equiv 360 \equiv 57 \mod 101$

   $11^{10} \equiv (11^4)^2 \times (11^2) \equiv (-4)^2 \times 20 \equiv 16 \times 20 \equiv 320 \equiv 17 \mod 101$

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 $x^a \mod q$.

$11^{13} \equiv 11^{10} \times 11^3 \equiv 17 \times 18 \equiv 306 \equiv 3 \mod 101$.

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

$11^{20} \equiv (11^{10})^2 \equiv (17)^2 \equiv 289 \equiv 87 \mod 101$

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

You have a choice whether to start with Alice's key, or Bob's key. Alice's key seems easier:

$$3^{20} \equiv (3^4)^5 \equiv (81)^5 \equiv (-20)^5 \equiv -3200000 \equiv 84 \mod 101$$

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

$x = 10$ does not generate all values modulo 101.

Notice, $10^2 \equiv 100 \mod 101$; $10^3 \equiv 91 \mod 101$; $10^4 \equiv 1 \mod 101$; and $10^5 \equiv 10 \mod 101$. And from here the pattern repeats.

Alternatively, notice, $10^2 \equiv 100 \equiv -1 \mod 101$. So $10^4 \equiv (-1)^2 \equiv 1 \mod 101$. Then $10^{4n} \equiv 1 \mod 101$ for all integers n.