Diffie-Hellman Worksheet

We'll fix a modulus $P = 257$ (which is prime), and a number $N = 3$.

1. You pick your secret exponent $a =$ _____. It should be an **odd** number between 3 and 255.

2. Find all powers of N modulo P listed below, reducing mod P after every step:

   (a) $N \pmod P =$ _____

   (b) $N^2 \pmod P =$ _____

   (c) $N^4 \pmod P =$ _____

   (d) $N^8 \pmod P =$ _____

   (e) $N^{16} \pmod P =$ _____

   (f) $N^{32} \pmod P =$ _____

   (g) $N^{64} \pmod P =$ _____

   (h) $N^{128} \pmod P =$ _____

3. Now find the powers above that sum to a, and compute $A = N^a \pmod P$ by multiplying those powers of N together. For example, if $a = 113$, then $a = 64 + 32 + 16 + 1$. So
$$A = N^a \pmod P = N^{64} \cdot N^{32} \cdot N^{16} \cdot N^1 \pmod P.$$

4. Trade your value of A with another person (and call theirs B).

5. Now compute $B^a \pmod P$ by the same repeated squaring method.

   (a) $B \pmod P =$ _____

   (b) $B^2 \pmod P =$ _____

   (c) $B^4 \pmod P =$ _____

   (d) $B^8 \pmod P =$ _____

   (e) $B^{16} \pmod P =$ _____

   (f) $B^{32} \pmod P =$ _____

   (g) $B^{64} \pmod P =$ _____

   (h) $B^{128} \pmod P =$ _____

6. $B^a \pmod P$ is the secret number you have with the other person!

7. Now, choose a message to encrypt (1 - 2 sentences), and use the text on the page number "$B^a \pmod{P}$" in our textbook as your (common) secret key. Bring your encrypted message for your partner next time. They will then try to decrypt it using your common secret key. You will also get a message from them to decrypt!