Name:_____

Introduction to Cryptography
Multiplicative Cipher - Revisited

(1) Write a function in Python that
   (a) accepts a lowercase message (string) and a multiplicative key (integer) as arguments;
   (b) checks that the key is valid (mod 26);
   (c) performs the multiplicative encryption to each letter modulo 26;
   (d) returns the encrypted message.

(2) Write a function in Python that
   (a) accepts a plaintext integer, multiplicative key (integer), and a modulus n (integer) as arguments;
   (b) checks that the key is valid (mod n);
   (c) checks that the modulus is larger than the plaintext integer;
   (d) performs the multiplicative encryption to the integer modulo n;
   (e) prints the encrypted integer.

(3) By hand, encrypt the number 14 with a modulus of 13 and a multiplicative key of 2. By hand, encrypt the number 1 with a modulus of 13 and a multiplicative key of 2. What happens if the modulus is less than or equal to the plaintext integer?

(4) Use your function from problem 2 to encrypt the number 1234567 by multiplying by the key $A = 319765$ using the modulus 27989898.

(5) Let A be an integer. A **multiplicative inverse of A mod n** is an integer x such that $Ax \equiv 1 \mod n$.
   (a) Let $A = 2$. Test each value of x where $0 \leq x \leq 25$ and determine whether there exists a multiplicative inverse of A modulo 26 (please don't do this manually).
   (b) Repeat the above exercise for each value of A where $0 \leq A \leq 25$ (please don't do this manually).
   (c) Make a conjecture regarding which values of A have a multiplicative inverse modulo 26.
   (d) Make a conjecture regarding which values of A have a multiplicative inverse modulo n.

(6) Verify that the multiplicative inverse of $A = 319765$ is 27698239 modulo 27989898. How can this be used to decrypt your answer in problem 4?