Name:_____

Introduction to Cryptography
Multiplicative Cipher

(1) Write a program in Python that
   (a) prompts the user for a lowercase message;
   (b) prompts the user for a multiplicative key;
   (c) performs the multiplicative encryption to each letter modulo 26;
   (d) prints the encrypted message.
(2) Suppose your message is the string "abcdefghijklmnopqrstuvwxyz". Write a program which uses a for-loop to perform the multiplicative cipher to this message for each key from 0 to 25. Which of these keys makes the encrypted alphabet a valid substitution cipher? Make a conjecture about the relationship between the valid keys and the number 26.
(3) Rather than encrypting each letter individually, we can instead encrypt blocks of letters simultaneously to provide more security. As an example, the plaintext message "fatcat" can be decomposed into two-letter blocks as "fa" "tc" "at". Using our usual scheme, the block "fa" is associated with the number 500, the block "tc" is associated with the number 1902, and the block "at" is associated with the number 19. What are we doing to accomplish this transformation? Encrypt each of these blocks by multiplying by 11 $\mod 2800$. What do you notice if you instead multiplied by 1400 $\mod 2800$?
(4) Suppose A and n are integers so that $Ax \equiv 0 \mod n$ for some integer $x \not\equiv 0 \mod n$. Make a conjecture about the relationship between A and n. If A is interpreted as a multiplicative key, conjecture when A will be a valid key.
(5) Compute the greatest common divisor of 234 and 500.
(6) Compute the greatest common divisor of 1331 and 2431.