A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
T	H	E	Q	U	I	C	K	B	R	O	W	N	F	X	J	M	P	D	V	L	A	Z	Y	G	S

1. The message below was encoded using the scheme shown above. Decode the original message. VKBD BD VKU EXPPUEV TFDZUP

2. Use the scheme above to encode the message "I LOVE YOU."

3. Let $p = 7$ and $q = 17$. Are p and q both prime numbers? Find $(p-1)(q-1)$, the number we call m. Now let e equal 5. Does e have any factors in common with m? Finally, verify that $77e - 4m = 1$.

4. Let $p = 5$ and $q = 19$. Are p and q both prime numbers? Find $(p - 1)(q - 1)$, the number we call m. Now select e to equal 11. Does e have any factors in common with m? Now suppose $d = 59$ and $y = 9$. Verify that $e \times d - m \times y = 1$.

5. Reduce the following : $1^2 \bmod 3$; $2^2 \bmod 3$; $3^2 \bmod 3$; $4^2 \bmod 3$; $5^2 \bmod 3$; $6^2 \bmod 3$. Do you notice a pattern?

6. Compute $2^4 \pmod 5$. Compute $4^4 \pmod 5$. Compute $3^4 \pmod 5$. Oh, what the heck, compute $n^4 \pmod 5$ for all numbers n from 1 through 4.

7. In our discussion, the two public numbers 7 and 143 were given. How would you encode the message "4"? The secret decoding number is 103. Without performing the calculation (unless you have a computer that can do modular arithmetic for you), how would you decode the encrypted message you just made if you were the receiver?

8. Suppose you wish to devise an RSA coding scheme for yourself. You select $p = 3$ and $q = 5$. Compute m, and then find (by trial and error if necessary) possible values for e and d.

9. Given the coding scheme you devised in the previous problem, show how a friend would encode "HI" (use 01 for A, 02 for B, . . . , 26 for Z to convert the letters to numbers). Now decode the coded message. Did you return to your original HI?

Use the following table as needed to solve the next few problems:

$73^7 \equiv 83 \bmod 143$	$83^{143} \equiv 58 \bmod 103$	$8^{103} \equiv 83 \bmod 143$
$74^7 \equiv 35 \bmod 143$	$74^{143} \equiv 51 \bmod 103$	$74^{103} \equiv 61 \bmod 143$
$61^7 \equiv 74 \bmod 143$	$38^{143} \equiv 29 \bmod 103$	$83^{103} \equiv 73 \bmod 143$
$83^7 \equiv 8 \bmod 143$	$35^{143} \equiv 5 \bmod 103$	$38^{103} \equiv 103 \bmod 143$
$38^7 \equiv 25 \bmod 143$	$8^{143} \equiv 72 \bmod 103$	$35^{103} \equiv 74 \bmod 143$

10. Using the list above, with the public numbers 7 and 143, how would you encode "83"? How would you decode the message using the decoding' number 103? What numbers in the list must you refer to for the encoding and decoding operations?

11. Using the list above, with the public numbers 7 and 143, how would you encode "61"? How would you decode the message using the decoding' number 103? What numbers in the list must you refer to for the encoding and decoding operations?

12. Using the list above, with the public numbers 7 and 143, and decoding number 103, how would you decode "38"? What numbers in the list must you refer to for this decoding operation?

13. Compute 5^{600} (mod 7). Compute $8^{1,000,000}$ (mod 11).

14. Recall how exponents work, for example, $7^{15} = 7^{(12+3)} = 7^{12} \times 7^3$. Now, using exponent antics, compute 5^{668} (mod 7).

15. Suppose that p is a prime number and n is a number that has p as a factor. What is n^{p-1} mod p in this case?

16. Compute 1^5 mod 6, 2^5 mod 6, 3^5 mod 6, 4^5 mod 6, and 5^5mod 6. What if you raise the numbers to the power 2? Compute n^6 mod 9 for numbers n from 1 to 8. What is the answer when n and 9 have no common factors? Do you think there is a way to extend Fermat's Little Theorem when the mod number is not prime? Make a guess (yes or no).

17. If you could factor a large public number into its two prime factors, how could you break the code? Outline the procedure.