Notes on the RSA Algorithm (a.k.a. "RIZZ"):

Exercises for Part A: SOLUTIONS.

1. Divide the positive integer $m = 5$ into each of the integers $a = 28$, $a = 300$, $a = 0$, $a = 1$, $a = -28$, and $a = -45$. That is, write each of these integers a in the form $a = m \cdot q + r$, where q and r are integers and $0 \leq r < m$. (You can probably do this by hand, but use a calculator if it helps.)

$$28 = 5 \cdot 5 + 3$$
$$300 = 5 \cdot 60 + 0$$
$$0 = 5 \cdot 0 + 0$$
$$1 = 5 \cdot 0 + 1$$
$$-28 = 5 \cdot (-6) + 2$$
$$-45 = 5 \cdot (-9) + 0$$

2. Repeat Exercise 1 above with $m = 2$ (and the same values of a).

$$28 = 2 \cdot 14 + 0$$
$$300 = 2 \cdot 150 + 0$$
$$0 = 2 \cdot 0 + 0$$
$$1 = 2 \cdot 0 + 1$$
$$-28 = 2 \cdot (-14) + 0$$
$$-45 = 2 \cdot (-23) + 1$$

3. Fill in each of the following two blanks with a single-word adjective: if the remainder of the integer a, upon division by 2, is 0, then a is an ____even____ integer; if the remainder is 1, then a is an ____odd____ integer.

4. For this exercise, recall the following, from Part A above: if a and d are integers, we say d *divides* a*, and write* $d|a$, if d goes into a evenly, meaning $a = d \cdot q$ for some integer q.

   (a) In other words, to say $d|a$ is to say that the remainder you get when you divide d into a is ____zero____. (Fill in the blank.)

(b) For which of the integers a, in Exercise 1 above, is it true that 5 divides a?
$a = 300$, $a = 0$, and $a = -45$.

(c) For which of the integers a, in Exercise 1 above, is it true that 2 divides a?
$a = 28$, $a = 300$, $a = 0$, and $a = -28$.

(d) For which of the integers a, in Exercise 1 above, is it true that 5 divides a *and* 2 divides a?
$a = 300$ and $a = 0$.

(e) For which of the integers a, in Exercise 1 above, is it true that 5 divides a *and* 15 divides a?
$a = 300$, $a = 0$, and $a = -45$.

(f) Is it always true that, if $d|a$ and $c|a$, then $cd|a$? Please explain.
No. $5|(-45)$ and $15|(-45)$, but $75 \nmid (-45)$.

5. (a) Which integers m, if any, satisfy $m|0$? Please explain.
Any integer m does, since $0 = m \cdot 0$ for any integer m.

(b) Which integers m, if any, satisfy $0|m$? Please explain.
The only integer that 0 divides is $m = 0$, because for 0 to divide m, we would need $0 \cdot c = m$ for some integer c, but the left hand side is always 0, so the right hand side must be 0 too.

You'll need a calculator for the following exercises.

6. (a) Numerize the single-letter message "L," using the numerization key above. Call your numerization n: $n =$ 22 .

(b) Compute n^k, with $k = 5$. Just plug n^k into your calculator, and write down the number you get. Answer: $n^k =$ 5,153,632 .

(c) Let $m = 577$. Find integers q and r, with $0 \leq r < m$, such that $n^k = m \cdot q + r$. Hint: first plug n^k/m into your calculator, and write your answer in decimal form:

$n^k/m =$ 8931.771231 .

Your answer should have some stuff to the left of the decimal, and some stuff to the right: that is, your answer should look like $q.y$ (the dot here indicates a decimal point, not a product), where q and y are positive integers. Then q *is* your quotient q. To find your remainder r, compute $m \cdot q$ and subtract it from n^k.
Write your answer here:

$$n^k = 577 \cdot 8931 + 445.$$

7. Repeat problem 1 with the message "A," the exponent $k = 7$, and the divisor $m = 223$:

$n =$ ___11___; $n^k =$ ___19,487,171___;

$n^k/m =$ ___87,386.41704___;

$n^k = 223 \cdot$ ___87,386___ $+$ ___93___.

8. Repeat problem 1 with the message "ME," the exponent $k = 2$, and the divisor $m = 1137$:

$n =$ ___2,315___; $n^k =$ ___5,359,225___;

$n^k/m =$ ___4,713.478452___;

$n^k = 1137 \cdot$ ___4,713___ $+$ ___544___.
