Math 345 – Wednesday 11/01/17

Exercise 35. Decode the following message, which was sent using the modulus $n = 7081$ and the exponent $k = 1789$. (Note that you will first need to factor n.)

$$5192, \quad 2604, \quad 4222$$

Exercise 36. It may appear that RSA decryption does not work if you are unlucky enough to choose a message a that is not relatively prime to n. Of course, if $n = pq$ and p and q are large, this is very unlikely to occur. [See Exercise 34.]

(a) Show that in fact RSA decryption does work for all messages a, regardless of whether or not they have a factor in common with n. In other words, show that RSA decryption works for all messages a as long as n is a product of distinct primes.

(b) Give an example with $n = 18$ and $a = 3$ where RSA decryption does not work. [Remember, k must be chosen relatively prime to $\phi(n) = 6$.]