Worksheet #10; date: 10/01/2018
MATH 55 Discrete Mathematics

1. Using Fermat's little theorem to find the inverse of 5 modulo 17.
2. *(Rosen 4.4.39)*
   (a) Use Fermat's little theorem to compute $5^{2003} \mod 7$, $5^{2003} \mod 11$ and $5^{2003} \mod 13$.
   (b) Use your results from part (a) and the Chinese remainder theorem to find $5^{2003} \mod 1001$. (Note that $1001 = 7 \cdot 11 \cdot 13$.)
3. *(Rosen 4.4.23)* Show that we can easily factor n when we know that n is the product of two primes, p and q, and we know the value of $(p-1)(q-1)$.
4. *(Rosen 4.4.25; modified)* Encrypt the message UPLOAD using the RSA system with $n = 53 \cdot 61$ and $e = 17$, translating each letter into integers and grouping together pairs of integers, as done in Example 8.
5. Knowing that $n = 53 \cdot 61$. What is the decryption key in the question above?