# HOMEWORK #3 – MATH 5405
# SPRING 2016

DUE: TUESDAY 2/22/2016

(1) Suppose you are given the block of data (16 bytes) consisting of all zeroes. Compute what the output of the
   (a) `ByteSub` on that data?
   (b) What is the output of `ShiftRow` on the output of `ByteSub` from (a)? (Please use the description of shiftrow from the text, in particular, still output a matrix).
   (c) What is the output of `MixColumn` on the output of `ShiftRow` from (b)?
   (d) Suppose that the roundkey for this round is made of all 1s. What is the output of the AddRoundKey phase. Provide a list of 16 bytes (numbers).

(2) Do Exercise 3 from pages 162-163 of the text Trappe and Washington.

(3) Do Exercise 4 from page 163 of the text Trappe and Washington.

(4) Do Exercise 5 from page 163 of the text Trappe and Washington.

(5) Let's describe one more factorization algorithm (you can even implement it before class on March 10th). This is called Pollard's Rho. If $p$ is a factor of $n$ then the expectation is that this will usually find a factor of $n$ in some constant times $\sqrt{p}$ steps.
   (a) Lookup the birthday problem on the internet and find an answer the following question. How many randomly chosen numbers $x_i$ in the range $0, \ldots, n-1$ are required so that there is at least a 50% probability that $x_i = x_j$ for some $i \neq j$. You don't need to prove that your answer is right.
   (b) The idea for us now we create a list of "random" numbers less than $n$. We do this by picking a polynomial $g(x)$ (usually $g(x) = x^2 + 1$), and then setting

$$x_1 = 2, x_2 = g(x_1) \bmod n, \ldots, x_{i+1} = g(x_i) \bmod n, \ldots$$

   We want to quickly find $i$ and $j$ where $x_i \equiv_p x_j$ so that $d = \gcd(x_i - x_j, n) > 1$. First define a new sequence $y_i$ as follows.

$$y_1 = x_1 = 2, y_2 = g(g(y_1)) \bmod n, y_3 = g(g(y_2)) \bmod n, \ldots, y_{i+1} = g(g(y_i)) \bmod n, \ldots$$

   Prove the following.

   **Claim:** *If $t$ and $l$ are the smallest integers such that $x_t \equiv_p x_{t+l}$ (and hence $x_t = x_{t+2l} = x_{t+3l} = \ldots$), then $x_i \equiv_p y_i$ in at most $t + l$ steps.*

   *Hint:* What is $y_i$ in terms of $x_i$. Try setting $i = t + l - (t \bmod l)$ and showing that $x_i = x_{2i}$.
   (c) Now define the sequences $x_i$ and $y_i$ as in part (b). If $x_i \equiv_p y_i$ how could you use that to find find a factor $p$ of $n$?
   (d) Write pseudo-code for that uses the above method to find factors of $n$.