Homework 2

Instructions: Submit typed solutions to these problems. For problems 1 and 2, submit your source code along with sample output of your choosing.

1. Write a function which takes as input two integers a and n, with $n \geq 0$ and returns the value of $\gcd(a, n)$ using the Euclidean Algorithm.

   It is not required that you validate the input to this function; that is, you may assume that both input parameters will, in fact, be integers, and that n will be positive.

2. Write a function which takes as input two integers a and n, with $n \geq 0$ and uses the Extended Euclidean Algorithm to return the multiplicative inverse of a mod n if such an inverse exists.

   As in problem 1, your code does not need to validate that your inputs are positive integers, but you *do* need to check that $\gcd(a, n) = 1$ and return an error if a and n are not relatively prime.

3. The following was encrypted by the Vigenère method. Decrypt it. Carefully document your work—in general, more details are better than fewer details. In particular, document how you determine the key length.

   ```
   XKJUROWMLLPXWZNPIMBVBQJCNOWXPCCHHVVFVSLLFVXHAZITYXOHULX
   QOJAXELXZXMYJAQFSTSRULHHUCDSKBXKNJQIDALLPQSLLUHIAQFPBPC
   IDSVCIHWHWEWTHBTXRLJNRSNCIHUVFFUXVOUKJLJSWMAQFVJWJSDYLJ
   OGJXDBOXAJULTUCPZMPLIWMLUBZXVOODYBAFDSKXGQFADSHXNXEHSAR
   UOJAQFPFKNDHSAAFVULLUWTAQFRUPWJRSZXGPFUTJQIYNRXNYNTWMHC
   ```

   The key for this encryption is a sequence of letters which form a recognizable pattern, even though they don't form a word.

4. You are an anthropologist studying on location an isolated language that has only the letters K, O, and Z. Previous studies have indicated that the index of coincidence for this language is about 0.37.

   A village merchant offers to sell you three rare manuscripts, and you can read their titles:

   ```
   "OOK OOK ZOOK"
    "OK KOZ KOZZ"
   "ZOKO ZOKO OOK"
   ```

   Your trusty guide warns you that one of the manuscripts is an illiterate and unreadable forgery. Knowing only the titles of these manuscripts, identify with explanation the one most likely to be forged.

5. Using a Playfair cipher with the following array as the key,

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

   encrypt the message "He deceived me."

6. From your linear algebra classes, you might remember that the inverse of a 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is given by $\dfrac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, provided that the determinant $ad - bc$ is non-zero.

   The formula for the inverse of a 2×2 matrix in $\mathbb{Z}_{26}$ is almost the same, except that (once again!) since we cannot divide in $\mathbb{Z}_{26}$, we have to multiply by an inverse instead. The inverse of a 2×2 matrix in $\mathbb{Z}_{26}$ is $(ad-bc)^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, provided that $\gcd(ad - bc, 26) = 1$.

   Compute the inverse of these matrices mod 26. (We will need to be able to do this during week 3!)

   (a) $\begin{bmatrix} 2 & 5 \\ 1 & 16 \end{bmatrix}$ (b) $\begin{bmatrix} 3 & 17 \\ 2 & 5 \end{bmatrix}$