Homework 4

Instructions: Submit answers to questions 1 and 2. I will not collect or grade problems 3 and 4 (the coding problems) at this time, but *save your code*, because these are the first two functions you'll need for AES!

1. Determine the involutory keys in the affine cipher mod 26.
2. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 4 & 2 & 8 & 6 & 5 & 9 & 1 \end{pmatrix}$

   (a) Write σ in one-row (cycle) notation.

   (b) What is the cycle type of σ?

   (c) Write σ as a composition of (not necessarily disjoint) transpositions.

   (d) Is σ an even permutation or an odd permutation?

   (e) Is σ an involution?

   (f) Now, let $\alpha = (1\ 4\ 8\ 5)\,(1\ 3\ 6\ 7)\,(2\ 9)$. Compute the conjugate of σ by α.

   (g) Is $\sigma\alpha\sigma\alpha^{-1}$ of matched cycle type? Explain why or why not.