1. The ciphertext QCZIAPWO has been generated with a shift cipher. Determine the key and the plaintext.

2. Show that the encryption key of a cryptosystem is always injective, i.e. if $e_k(x) = e_k(y)$, then $x = y$. [Hint: try decrypting.]

3. Show that the following defines a cryptosystem. Let $w$ be a string of English letters. Choose two shift cipher keys $k_1$ and $k_2$. Encrypt the elements of $w$ in odd places with $k_1$ and those in even places with $k_2$. Then reverse the encrypted string.

   Determine the set of plaintexts $P$, the set of ciphertexts $C$, and the set of keys $K$. [Hint: we did one like this in class.]

4. Use the affine cipher $e_k(x) = 3x + 1$ to encipher GAMECOCKS. What is the decrypting function $d_k(x)$?

5. Find the affine cipher (if it exists) that encrypts the plaintext BC into the ciphertext AD.