HOMEWORK 1, DUE FEB 6.

1. The ciphertext SEOYKJOEJ 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. Use the affine cipher $e_k(x) = 3x + 1$ to encipher BADGERS. What is the decrypting function $d_k(x)$?

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

5. Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher. Is there any advantage to doing this, rather than using a single affine cipher? Why or why not? [Hint: if e.g. $f(x) = 3x + 1$ and $g(x) = 5x + 2$, what does $f(g(x))$ look like?]