Math373 **Quiz 6** **Fri. Feb 21, 2014**

Name: ______________________________

Directions: Show all work. No credit for answers without work.

1. [**3 points**] Describe what it means for a symmetric cipher to be immune to a chosen plaintext attack.

2. Recall the multiplicative cipher: $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{F}_p^*$ and

$$e_k(m) = k \cdot m \qquad\qquad d_k(c) = k^{-1} \cdot c.$$

   (a) [**3 points**] Alice and Bob choose $p = 17$ and $k = 2$. Encrypt the message 12, and decrypt the ciphertext 15.

(b) [**4 points**] Alice and Bob choose $p = 53$ and select a secret key. Eve intercepts the ciphertext 10 and manages to recover the plaintext message 14. Find the key that Alice and Bob have selected.