Math373 **Quiz 6** **Fri. Feb 24, 2023**

Name: ____________________________________

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

1. **[3 parts, 2 points each]** Consider the affine cipher with key $k = (\alpha, \beta)$ whose functions are given by $e_k(m) = \alpha m + \beta$ and $d_k(c) = \alpha^{-1}(c - \beta)$ in $\mathbb{Z}_m$.

   (a) Specify the key space for this cipher as a product $A \times B$, where A is the set of all candidates for α and B is the set of all candidates for β.

   (b) Let $m = 38$, and let $k = (\alpha, \beta) = (15, 6)$. Decrypt the ciphertext $c = 22$.

   (c) Eve obtains the plaintext/ciphertext pairs $(10, 22)$ and $(15, 25)$. Find the key (α, β).

2. **[2 parts, 2 points each]** Alice and Bob meet privately and decide to communicate using the exclusive-or cipher with a block size of 6 bits. They agree on a private key k.

   (a) Alice sends the first ciphertext $c_1 = 100110$ to Bob, which Eve intercepts. What can Eve conclude about the corresponding plaintext message m_1? Explain.

   (b) Bob responds to Alice with the second ciphertext $c_2 = 011101$, which Even intercepts. What can Eve conclude about the corresponding plaintext messages m_1 and m_2? Explain.