Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. [JJJ 1.41] Consider the affine cipher with key $k = (\alpha, \beta)$ whose encryption and decryption functions are given by

$$e_k(m) \equiv \alpha m + \beta \pmod{p}$$
$$d_k(c) \equiv \alpha^{-1}(c - \beta) \pmod{p}$$

   (a) Let $p = 541$ and let $k = (34, 71)$. Encrypt the message $m = 204$. Decrypt the ciphertext $c = 431$.

   (b) Assuming that p is public knowledge, explain why the affine cipher is vulnerable to a chosen plaintext attack. How many plaintext/ciphertext pairs are likely to be needed to recover the private key?

   (c) Alice and Bob decide to use the prime $p = 601$ for their affine cipher. The value of p is public knowledge. Eve intercepts the ciphertexts $c_1 = 324$ and $c_2 = 381$, and she also manages to discover that the corresponding plaintexts are $m_1 = 387$ and $m_2 = 491$. Determine the private key (α, β) and then use it to encrypt the message $m_3 = 173$.

2. [JJJ 1.43] Let n be a large integer and let $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{Z}_n$. For each of the functions below, answer the following questions.

   - Is e an encryption function? In other words, can we always recover the plaintext $m \in \mathcal{M}$ given $e_k(m)$, or are there distinct m_1 and m_2 such that $e_k(m_1) = e_k(m_2)$? (Or, for the mathematically inclined, we ask is $e_k \colon \mathcal{M} \to \mathcal{C}$ is an injective function?)
   - If e is an encryption function, what is the associated decryption function d?
   - If e is not an encryption function, can you make it into an encryption function by restricting the set of keys $\mathcal{K}$ to a smaller, but still reasonably large subset?

   (a) $e_k(m) \equiv k - m \pmod{n}$

   (b) $e_k(m) \equiv k \cdot m \pmod{n}$

   (c) $e_k(m) \equiv (k + m)^2 \pmod{n}$

3. [JJJ 1.46] Explain why the exclusive-or cipher is not secure against a chosen plaintext attack. Demonstrate the attack by computing the key given the plaintext/ciphertext pair with $m = 1100101001$ and $c = 0011001100$).

4. [JJJ 1.48] Why modular arithmetic? Alice and Bob decide to use a multiplicative cipher that does not involve modular arithmetic. That is, they use $\mathcal{K} = \{p \colon p \text{ is a prime}\}$, $\mathcal{M} = \mathcal{C} = \{1, 2, 3, \ldots\}$, and

$$e_k(m) = km \qquad\qquad d_k(c) = c/k.$$

   Eve intercepts the following ciphertexts:

$$c_1 = 19157632841654891 \qquad c_2 = 39493517444969867 \qquad c_3 = 32351977451572789$$

   Illustrate that this cipher lacks property (3) by finding the key k.