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

1. [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 $c = 0011001100$).

2. [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. *Hint:* it may be useful to use sage or another mathematical computational package.

3. Modular exponentiation cipher. Consider the cipher where $\mathcal{K}$ is the set of primitive roots in $\mathbb{F}_p$, $\mathcal{M} = \mathbb{Z}_{p-1}$, $\mathcal{C} = \mathbb{F}_p^*$, and $e_k(m) = k^m$.

   (a) Alice and Bob choose $p = 11$ and $k = 2$. Encrypt the message 6 and decrypt the message 3.

   (b) Prove that the encryption function is injective, and describe the decryption function.

   (c) Does this cipher have property (1) (i.e. given $k \in \mathcal{K}$ and $m \in \mathcal{M}$, it is easy to compute $e_k(m)$)? Does it have property (2) (i.e. given $k \in \mathcal{K}$ and $c \in \mathcal{C}$, it is easy to compute $d_k(c)$)?

   (d) Here, we illustrate that this cipher is vulnerable to a chosen plaintext attack. Alice and Bob choose $p = 2687$ and a secret key. Eve manages to discover the plaintext/ciphertext pairs $(1866, 1864)$ and $(1231, 2565)$. Find the secret key.

4. The Discrete Logarithm. Evaluate the following in $\mathbb{F}_{23}$.

   (a) $\log_{14}(22)$

   (b) $\log_{15}(8)$

5. Diffie–Hellman Key Exchange. Alice and Bob select and publish

$$p = 918398656403699$$
$$g = 581330380946540.$$

   (a) Alice selects the secret integer $a = 382114$. Compute $A = g^a$. Alice sends A to Bob.

   (b) Bob selects the secret integer $b = 1744891346$. Compute $B = g^b$. Bob sends B to Alice.

   (c) What modular computation does Alice perform to obtain the shared secret? As Alice, compute the shared secret.

   (d) What modular computation does Bob perform to obtain the shared secret? As Bob, compute the shared secret.