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

1. The Discrete Logarithm. Evaluate the following in $\mathbb{F}_{23}$.
   (a) $\log_{14}(22)$
   (b) $\log_{15}(8)$

2. 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 $e_k(m) = k^m$ in $\mathbb{F}_p$.
   (a) Alice and Bob choose $p = 11$ and $k = 2$. Find the order of k in $\mathbb{F}_p$. Is k a primitive root? 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 k.
   (e) In part (d), the intention is to find the secret key k by using an efficient attack, but the numbers are small enough that you could find k using brute force. Carry out the attack again with p and plaintext/ciphertext pairs (m_1, c_1), (m_2, c_2) as shown below.

$$\begin{aligned} p &= 49651418153203334334343025759447351841028834755961145327 \\ m_1 &= 1442506475715854841019941447847762099575753178605423941 \\ c_1 &= 11799308873252204640351057233329997891282186998411681189 \\ m_2 &= 8741291516595786171636620315162766721085153317204173630 \\ c_2 &= 35688851452468689917269021024163741705031317552447325666 \end{aligned}$$

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

$$\begin{aligned} p &= 918398656403699 \\ g &= 581330380946540. \end{aligned}$$

   (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.