Name: _____

Directions: Show all work unless directed otherwise. No credit for answers without work.

1. **[5 points]** Give the definition of a prime number.

2. **[5 points]** Compute $\text{ord}_7(27440)$.

3. **[15 points]** Compute $(26)^{-1}$ in $\mathbb{F}_{71}$ using the fast power algorithm. Show all work in your computation.

4. **[15 points]** Let p be a prime and let s, t, and a be integers such that $p \nmid a$. Prove that if $s \equiv t \pmod{p-1}$, then $a^s \equiv a^t \pmod{p}$.

5. Primitive roots in $\mathbb{F}_{19}$.

   (a) **[5 points]** Verify that 2 is a primitive root in $\mathbb{F}_{19}$ using as few modular exponentiation computations as possible.

   (b) **[5 points]** Use part (a) to find all primitive roots in $\mathbb{F}_{19}$.

6. **[15 points]** Alice and Bob decide to use the affine cipher in $\mathbb{F}_{79}$. Recall that $\mathcal{K}$ is the set of pairs (α, β) in $\mathbb{F}_{79}$ such that $\alpha \neq 0$, $\mathcal{M} = \mathcal{C} = \mathbb{F}_{79}^*$, and

$$e_k(m) = \alpha m + \beta \qquad\qquad d_k(c) = \alpha^{-1}(c - \beta).$$

Suppose that Eve intercepts ciphertexts $c_1 = 8$ and $c_2 = 56$ and discovers that the corresponding messages are $m_1 = 61$ and $m_2 = 54$. Find Alice and Bob's shared key (α, β).

7. **[3 parts, 5 points each]** Recall the exclusive-or cipher, where $\mathcal{K}$, $\mathcal{M}$, and $\mathcal{C}$ are the set of bitstrings of length B, and $e_k(m) = k \oplus m$.

   (a) What is the decryption function $d_k(c)$?

   (b) Alice and Bob use $k = 10011$. Encrypt 00101 and decrypt 11101.

   (c) Alice and Bob decide to use the exclusive-or cipher, and agree on a shared key k which is not known to Eve. Alice selects a message m, computes $c = e_k(m)$, and sends c to Bob. Unfortunately, Eve intercepts c. Is the cipher secure? Explain why or why not.

8. **[5 points]** Describe the relative difficulty of the Discrete Logarithm Problem (DLP) and the Diffie-Hellman Problem (DHP).

9. Alice and Bob use Diffie-Hellman to exchange a shared key. They choose $p = 47$ and $g = 15$.

   (a) **[7 points]** Alice chooses the secret integer $a = 12$. What should she send to Bob?

   (b) **[8 points]** Alice receives the reply 7 from Bob. What is the the shared key?

10. **[2 bonus points]** Instruction: phrase your response in the form of a question. Germany sent this encrypted message to Mexico in 1917 which discussed a plan for Mexico to attack the United States.