Name: Solutions

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

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

An integer n is prime if $n \geq 2$ and the only positive divisors of n are 1 and n.

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

$27440 = 7^3 \cdot 80$, where $7 \nmid 80$.

So $\mathrm{ord}_7(27440) = \boxed{3}$.

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

$(26)^{-1} = (26)^{71-2} = (26)^{69}$.

- $(26)^2 = 676 = 37$
- $(26)^4 = (37)^2 = 1369 = 20$
- $(26)^8 = (20)^2 = 400 = 45$
- $(26)^{16} = (45)^2 = 2025 = 37$
- $(26)^{32} = (37)^2 = 20$
- $(26)^{64} = (20)^2 = 45$

- $69 = 64 + 4 + 1$

$(26)^{69} = (26)^{64} \cdot (26)^4 \cdot (26) = 45 \cdot 20 \cdot 26 = \boxed{41}$

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 $a^s \equiv a^t \pmod{p}$.

Proof. If $s \equiv t \pmod{p-1}$, then $p-1 \mid s-t$, and $s-t = u(p-1)$ for some integer u. Hence

$$a^s \equiv a^{t+u(p-1)} \equiv a^t \cdot a^{u(p-1)} \equiv a^t \cdot (a^{p-1})^u \equiv a^t \cdot 1^u \equiv a^t$$

where we have that $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem. $\boxtimes$

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

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

Note that $19 = 2 \cdot 3^2$. We check $2^{18/2}$ and $2^{18/3}$.

- $2^9 = 512 = 18$
- $2^6 = 64 = 7$

$\}$ since both are not equal to 1, 2 is a primitive root of $\mathbb{F}_{19}$.

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

- Primitive roots have the form 2^k where $\gcd(k, 18) = 1$

k candidates: $\cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17$

Primitive roots: $2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$

$$\boxed{2,\ 13,\ 14,\ 15,\ 3,\ 10}$$

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).

54

$8 = \alpha \cdot 61 + \beta$

$- \quad 56 = \alpha \cdot 54 + \beta$

$-48 = \alpha(7)$

So $7\alpha = 31$.

We need $(7)^{-1}$ is 34. Mult both sides by 34:

Ext Euclid to find $(7)^{-1}$:

$79 = 11 \cdot 7 + 2$

$7 = 3 \cdot 2 + 1$

$1 = 7 - 3 \cdot 2$

$= 7 - 3(79 - 11 \cdot 7) = 34 \cdot 7 - 3 \cdot 79$

$(34)(7)\alpha = (31)(34)$

$\boxed{\alpha = 27}$

$\beta = 8 - \alpha \cdot 61 = 8 - (27)(61) = -1639$

$= -59 = 20$. So $(\alpha, \beta) =$

$\boxed{(27, 20)}$.

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 $d_k(c)$?

$d_k(c) = k \oplus c$

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

$e_k(00101) = 10110$

$d_k(11101) = 01110$

(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.

Yes, the cipher is secure; the ciphertext that Eve sees is consistent with all messages $m \in \mathcal{M}$. That is, for each $m \in \mathcal{M}$, there is a key $k \in \mathcal{K}$ such that encrypting m with k gives c.

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

DLP is at least as difficult as DHP: DLP $\geq$ DHP.
It is not known ~~if~~ whether they are equally difficult.

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?

Alice sends $g^a = (15)^{12} = ((15)^4)^3 = (50625)^3 =$

$= (6)^3 = 216 = \boxed{28}$.

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

The reply is $B = g^b$. Alice computes

$(B)^a = (7)^{12} = ((7)^4)^3 = (2401)^3 = (4)^3 = 64 = \boxed{17}$

as 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.

What is the Zimmermann Telegram?