Name: Solutions

Directions: Show all work, including fast power and extended Euclidean algorithm work, unless directed otherwise. No credit for answers without work.

1. Alice and Bob use the ElGamal cryptosystem to exchange messages with $p = 383$ and $g = 212$. Bob selects $b = 8$ as his private key and Alice publishes $A = 74$ as her public key.

   (a) **[~~7~~ 10 points]** What is Bob's public key?

   $B = g^b = (212)^8 = \boxed{62}$

   $212^2 = 133$

   $(212)^4 = 71$

   $(212)^8 = 71 \cdot 71 = 62$

   (b) **[9 points]** Bob wishes encrypt the message $m = 144$ and send to Alice. He chooses $k = 18$ as his ephemeral key. What ciphertext should he send to Alice?

   $C_1 = g^k$
   $= (212)^{18}$
   $= (212^8)^2 \cdot (212)^2$
   $= (62)^2 \cdot 133$
   $= 511252$
   $= 330$

   $C_2 = mA^k = 144 \cdot A^{16} \cdot A^2$

   $A^2 = 114$
   $A^4 = 357$
   $A^8 = 293$
   $A^{16} = 57$

   $= 144 \cdot 57 \cdot 114$
   $= 43$

   So he sends $\boxed{(330, 43)}$

   (c) **[~~9~~ 15 points]** Alice encrypts a message with Bob's public key and sends the ciphertext $(5, 211)$ to Bob. Find Alice's message to Bob.

   - $S = C_1^b = 5^8 = 5^4 \cdot 5^4 = (625)^2 = 348$

   - Compute S^{-1} in $\mathbb{F}_{383}$:

   $383 = 1 \cdot 348 + 35$
   $348 = 9 \cdot 35 + 33$
   $35 = 1 \cdot 33 + 2$
   $33 = 16 \cdot 2 + 1$

   $1 = 33 - 16 \cdot 2$
   $= 33 - 16(35 - 1 \cdot 33)$
   $= 17 \cdot 33 - 16 \cdot 35$
   $= 17(348 - 9 \cdot 35) - 16 \cdot 35$
   $= 17 \cdot 348 - 169 \cdot 35$
   $= 17 \cdot 348 - 169(383 - 348)$
   $= 186 \cdot 348 - 169 \cdot 383$

   - $m = S^{-1} \cdot C_2 = 186 \cdot 211 = \boxed{180}$

2. **[5 points]** Place the following six functions in order so that if $f(x)$ proceeds $g(x)$, then $f(x) = O(g(x))$. You do not need to show your work.

& more space.

$$x^2(\ln x)^5, x, e^x, x^5(\ln x)^2, \frac{1}{x}, 1$$

$$\frac{1}{x}, 1, x, x^2(\ln x)^5, x^5(\ln x)^2, e^x$$

3. Use Shanks's Algorithm to find an x such that $2^x \equiv 120 \pmod{223}$.

(a) **[8 points]** Compute List 1 from Shanks's Algorithm. ~~Show details for your first two entries~~; no details needed for the others. Hint: the order of 2 in $\mathbb{F}_{223}$ is 37.

$n = \lceil \sqrt{37} \rceil = 7$

i	0	1	2	3	4	5	6	7
g^{in}	1	128	105	60	98	56	32	82

(b) **[8 points]** Compute List 2 from Shanks's Algorithm. ~~You may stop as soon as you detect a collision with List 1.~~

j	0	1	2	3	4	5	6
hg^j	120	17	34	68	136	49	98

(c) **[4 points]** Use (a) and (b) to find a solution x.

$$g^{4\cdot 7} = h \cdot g^6$$

$$g^{28-6} = h$$

$$g^{22} = h$$

So $x = 22$ is a solution.

4. Let $M = 940$. Note that the prime factorization of M is $M = 2^2 \cdot 5 \cdot 47$.

   (a) **[5 points]** According to the Chinese Remainder Theorem (CRT), 812 in $\mathbb{Z}_M$ corresponds to a list (a, b, c) where $a \in \mathbb{Z}_4$, $b \in \mathbb{Z}_5$, and $c \in \mathbb{Z}_{47}$. What is this list?

$$(812 \bmod 4,\ 812 \bmod 5,\ 812 \bmod 47) = \boxed{(0, 2, 13)}$$

   (b) **[20 points]** Solve the following system of congruences.

$$\begin{aligned} x &\equiv 2 \pmod{4} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 43 \pmod{47} \end{aligned}$$

i	m_i	z_i	$y_i = z^{-1} \bmod m_i$	a_i
1	4	235	$(235)^{-1} = 3^{-1} = 3$	2
2	5	188	$(188)^{-1} = 3^{-1} = 2$	1
3	47	20	[illegible] -7	43

Find $(20)^{-1} \bmod 47$:

$47 = 2 \cdot 20 + 7$
$20 = 2 \cdot 7 + 6$
$7 = 1 \cdot 6 + 1$

$1 = 7 - 1 \cdot 6$
$= 7 - 1 \cdot (20 - 2 \cdot 7)$
$= 3 \cdot 7 - 1 \cdot 20$
$= 3(47 - 2 \cdot 20) - 1 \cdot 20$
$= 3 \cdot 47 - 7 \cdot 20$

Modulo 940:

$x \equiv 2 \cdot 3 \cdot 235 + 1 \cdot 2 \cdot 188 + 43 \cdot (-7) \cdot 20$

$\equiv 1410 + 376 - 6020$

$\equiv -4234$

$\equiv \cancel{4606 \bmod 940}$

$\equiv \boxed{466 \bmod 940}$

5. **[10 points]** Let d and m be positive integers such that d divides m. Prove that if $a \equiv b \pmod{m}$, then $a \equiv b \pmod{d}$.

Suppose that $a \equiv b \pmod{m}$. This means that $m \mid a-b$, so $a-b = mk$ for some integer k.

Since $d \mid m$, we know that $m = dl$ for some integer l.

Therefore $a-b = mk = (dlk) = (lk)\cdot d$ and it follows that $d \mid a-b$. This implies that $a \equiv b \pmod{d}$.

6. **[15 points]** Solve for x in $x^7 \equiv 2 \pmod{161}$. Hint: $161 = 7 \cdot 23$.

- $N' = 6 \cdot 22 = 132$.
- Find inverse d of 7 in $\mathbb{Z}_{132}$:

$132 = 18 \cdot 7 + 6$

$7 = 1 \cdot 6 + 1$

$1 = 7 - 1 \cdot 6$

$= 7 - 1(132 - 18 \cdot 7) = 19 \cdot 7 - 1 \cdot 132$

- $d \equiv 19 \mod 132$
- $x \equiv (2)^{19} \equiv (2^8)^2 \cdot 2^3 \equiv (256)^2 \cdot 8$

$\equiv (95)^2 \cdot 8 \equiv 72200 \equiv \boxed{72} \pmod{161}$