Math373 **Test 2** **Fri. Mar. 10, 2023**

Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[12 points]** Let $p = 409$ and note that p is prime. Use the fast power algorithm to compute $(219)^{81}$ in $\mathbb{F}_p$.

$(219)^2 = 219 \cdot 219 = 108$

$(219)^4 = (108)^2 = 212$

$(219)^8 = (212)^2 = 363$

$(219)^{16} = (363)^2 = 71$

$(219)^{32} = (71)^2 = 133$

$(219)^{64} = (133)^2 = 102$

$81 = 64 + 16 + 1$

$(219)^{81} = (219)^{64} \cdot (219)^{16} \cdot (219)$

$= 102 \cdot 71 \cdot 219 = 289 \cdot 219 = 63{,}291$

$= \boxed{305}$

2. **[2 parts, 7 points each]** Let $p = 269$ and note that p is a prime.

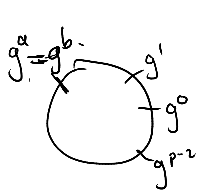
(a) What are the possible orders of elements in $\mathbb{F}_p$?

The orders divide $p-1$, and $p-1 = 268 = 2^2 \cdot 67$ prime

So the possible orders are $\boxed{1, 2, 4, 67, 134, \text{ and } 268}$ (all divisors of 268).

(b) Suppose that g is a primitive root in $\mathbb{F}_p$ and $g^a = g^b$ for some some integers a and b. What can we conclude about a and b?

Since g is a primitive root in $\mathbb{F}_p$, g has order $p-1$. So $g^0, g^1, \dots, g^{p-2}$ are all distinct elts in $\mathbb{F}_p^*$. It follows that $a-b$ is an integer multiple of $p-1$, and so $\boxed{a \equiv b \pmod{p-1}}$.



3. **[7 points]** Alice and Bob switch to the Exclusive-OR cipher with key $k = 100110$. Alice receives the ciphertext $c = 111000$. What is the corresponding plaintext?

$$m = k \oplus c = \begin{array}{r} 100110 \\ \oplus\ 111000 \\ \hline 011110 \end{array}$$

So the plaintext is $\boxed{011110}$.

4. **[7 points]** Let $p = 19$. Compute $\log_3(7)$.

n	0	1	2	3	4	5	6	7	8	9	....
3^n	1	3	9	8	5	15	7	2	6	18	

$\cdot 3$ $\cdot 3$ $\cdot 3$

Check: $1 \overset{?}{=} 3^{p-1} = 3^{18} = 3^{2\cdot 9} = (3^9)^2$
$= (18)^2 = (-1)^2 = 1$ ✓.

So $\log_3(7) = \boxed{6}$ in $\mathbb{F}_{19}$.

5. **[2 parts, 6 points each]** Alice and Bob use the Diffie Hellman secret key exchange protocol. They select $p = 587$ and $g = 2$. The following table of powers in $\mathbb{F}_p$ may be helpful.

n	1	2	4	8	16	32	64	128	256	512
$(2)^n$	2	4	16	256	379	413	339	456	138	260
$(184)^n$	184	397	293	147	477	360	460	280	329	233
$(417)^n$	417	137	572	225	143	491	411	452	28	197

(a) Bob chooses private number $b = 184$. What should he send to Alice?

He sends $B = g^b = 2^{184}$. We have $184 = 128 + 56 = 128 + 32 + 24$
$= 128 + 32 + 16 + 8$.

So $B = 2^{184} = 2^{128} \cdot 2^{32} \cdot 2^{16} \cdot 2^{8} = (456 \cdot 413) \cdot (379 \cdot 256) = 488 \cdot 169$
$= 82472 = \boxed{292}$

(b) Bob receives $A = 417$ from Alice. What is their shared secret key?

Shared secret is $g^{ab} = (g^a)^b = A^b = 417^{184} = 417^{128} \cdot 417^{32} \cdot 417^{16} \cdot 417^{8}$
$= (452 \cdot 491) \cdot (143 \cdot 225) = 46 \cdot 477 = \boxed{223}$

6. **[2 parts, 12 points each]** Alice and Bob use the ElGamal cipher, with $p = 227$ and $g = 5$. Alice picks $a = 28$ as her private key and in $\mathbb{F}_p$ computes $A = g^a = 49$ as her public key. Bob picks $b = 77$ as his private key and computes $B = g^b = 106$. The following table of powers in $\mathbb{F}_p$ may be helpful.

n	1	2	4	8	16	32	64	128
$(5)^n$	5	25	171	185	175	207	173	192
$(28)^n$	28	103	167	195	116	63	110	69
$(30)^n$	30	219	64	10	100	12	144	79
$(49)^n$	49	131	136	109	77	27	48	34
$(71)^n$	71	47	166	89	203	122	129	70
$(77)^n$	77	27	48	34	21	214	169	186
$(84)^n$	84	19	134	23	75	177	3	9
$(101)^n$	101	213	196	53	85	188	159	84
$(106)^n$	106	113	57	71	47	166	89	203

(a) Alice wishes to send Bob the message $m = 30$ and picks the random element $t = 84$. Using only information available to Alice, what does Alice send to Bob?

$c_1 = g^t = 5^{84}$. Note $84 = 64 + 20 = 64 + 16 + 4$.

$c_1 = 5^{84} = 5^{64} \cdot 5^{16} \cdot 5^4 = 173 \cdot 175 \cdot 171 = 63$

$c_2 = m g^{bt} = m B^t = m(106)^{84} = m\left(106^{64} \cdot 106^{16} \cdot 106^4\right) = (30 \cdot 89)(47 \cdot 57)$
$= 173 \cdot 182 = 160$

Alice sends $\boxed{(63, 160)}$ to Bob.

(b) Bob sends the ciphertext $(c_1, c_2) = (71, 100)$. Help Alice decrypt Bob's message.

- $c_1 = 71 = g^t$, $c_2 = 100 = mA^t = m g^{at} = m(g^t)^a = m(71)^{28}$
- $71^{28} = 71^{16} \cdot 71^8 \cdot 71^4 = 203 \cdot 89 \cdot 166 = 225$.
- $101 = m \cdot 225$. Need $(225)^{-1}$:

$227 = (1)(225) + 2$

$225 = (112)(2) + 1$

$1 = 225 + (-112)(2)$
$= 225 + (-112)[227 + (-1)(225)]$
$= (113)(225) + (-112)(227)$

- So $(225)^{-1} = 113$ and

$100 = m \cdot 225$

$(100)(113) = m \cdot 1$

$m = 100 \cdot 113 = \boxed{177}$

7. Let $p = 167$ and let $g = 24$. We use Shanks's baby-step/giant-step algorithm to compute $\log_g(7)$ in $\mathbb{F}_p$. Note that g has order 83 in $\mathbb{F}_p$, and we may take $n = 1 + \lfloor\sqrt{83}\rfloor = 10$.

(a) **[8 points]** Compute List 1 (the baby-steps).

n	0	1	2	3	4	5	6	7	8	9	10
g^n	1	24	75	130	114	64	33	124	137	115	88

$\cdot 24$

(b) **[12 points]** Compute List 2 (the giant-steps).

Need $g^{-10} = (g^{10})^{-1} = (88)^{-1}$.

$167 = (1)(88) + 79$
$88 = (1)(79) + 9$
$79 = (8)(9) + 7$
$9 = (1)(7) + 2$
$7 = (3)(2) + 1$

$1 = 7 + (-3)(2)$
$= 7 + (-3)(9 + (-1)(7))$
$= (4)(7) + (-3)(9)$
$= (4)[79 + (-8)(9)] + (-3)(9)$
$= (4)(79) + (-35)(9)$

$1 = (4)(79) + (-35)(88 + (-1)(79))$
$= (39)(79) + (-35)(88)$
$= (39)[167 + (-1)(88)] + (-35)(88)$
$= (39)(167) + (-74)(88)$

So $g^{-10} = 88^{-1} = -74 = 93$.

n	0	1	2	3	4	5	6	7	8	9
hg^{-nj}	7	150	89	94	58	50	141	87	75	128

$\cdot 93$ $\cdot 93$

(c) **[4 points]** If it exists, find $\log_g(7)$.

We see $75 = g^2 = h g^{-10 \cdot 8}$, so

$g^2 \cdot g^{80} = h$

$g^{82} = h$

So $\log_g(7) = \boxed{82}$.