CIS 3362 Sample Exam #3 Solutions
(taken from 2025 Quiz 4, 5)

1) (6 pts) Determine the Prime Factorization of 1,843,956,000.

Start by dividing out as many copies of 2, 3, 5, etc.

$1843956000 = 2^3 \times 5^3 \times 1843956 = 2^3 \times 5^3 \times 2^2 \times 3^2 \times 17 \times 3013$

$= 2^5 \times 3^2 \times 5^3 \times 17 \times 3013$

$= 2^5 \times 3^2 \times 5^3 \times 17 \times 23 \times 131$

Grading: 1 pt per term

2) (8 pts) Determine φ(1,843,956,000) **and give your answer in prime factorized form.**

$\varphi(1843956000) = \varphi(2^5) \times \varphi\ 3^2 \times \varphi(5^3) \times \varphi(17) \times \varphi(23) \times \varphi(131)$

$= (2^5 - 2^4)(3^2 - 3)(5^3 - 5^2)(17 - 1)(23 - 1)(131 - 1)$

$= 2^4 \times 2 \times 3 \times 5^2 \times 2^2 \times 2^4 \times 2 \times 11 \times 130$

$= 2^{12} \times 3 \times 5^2 \times 11 \times 2 \times 5 \times 13$

$= 2^{13} \times 3 \times 5^3 \times 11 \times 13$

Grading: 1 pt for breaking down by prime factor
3 pts for plugging in for each term based on each prime factor
4 pts for simplifying correctly to prime factorized form (give partial as needed)

If they answer 439296000 (answer multiplied out), award 6 of 8 points.

3) (6 pts) Determine the remainder when 47^{12208} is divided by 719. Note that 719 is prime. **For full credit use Fermat's Theorem.**

Since gcd(47, 719) = 1 and 719 is prime, $47^{718} \equiv 1 \pmod{719}$ via Fermat's Theorem.

$47^{12208} = 47^{17 \times 718 + 2} = (47^{718})^{17} \times 47^2 \equiv 1^{17} \times 2209 \equiv$ **52 (mod 719)**

Also accepted: $47^{12208} \equiv 47^{12208 \bmod 718} \equiv 47^2 \equiv 2209 \equiv$ **52 (mod 719)**, but only if they explicitly state which step (the mod in the exponent step) utilizes Fermat's Theorem.

2 pts for directly stating Fermat's Theorem or stating when it was used and using it correctly.

2 pts for reducing problem to 47^2 mod 719

2 pts for the correct answer

4) (6 pts) Determine the remainder when 48^{355743} is divided by 65219. **For full credit use Euler's Theorem.**

$65219 = 7^2 \times 1331 = 7^2 \times 11^3$

$\varphi(65219) = \varphi(7^2 \times 11^3) = \varphi(7^2) \times \varphi(11^3) = (7^2 - 7)(11^3 - 11^2) = 42 \times (1331 - 121) = 42 \times 1210 = 50820$

Since gcd(48, 65219) = 1, it follows that $48^{50820} \equiv 1 \pmod{65219}$ via Euler's Theorem.

$48^{355743} = 48^{50820 \times 7 + 3} = (48^{50820})^7 \times 48^3 \equiv 1^7 \times 110592 \equiv$ **45373 (mod 65219)**

Grading: 2 pts prime fact of 65219
2 pts for stating phi(65219)
2 pts to get to the correct answer
give an integer number of partial points as needed

5) (15 pts) We spend a good deal of class time on the discrete log problem. In particular, we covered an algorithm that utilizes $O(\sqrt{p})$ time and memory to solve the problem, which if faster

than the typical O(p) brute force solution. Utilize this technique to determine the value of x which satisfies the following equation:

$$2^x \equiv 6 \ (mod\ 101)$$

Specifically, please use increments of 11 for your stored memory. (So work out 2^{11}, 2^{22}, 2^{33}, ..., 2^{110} mod 101) and store these in the table provided below. Then, below that, show your incremental work until you get to the answer.

Exponent	2^{exp} mod 101
11	28
22	28 x 28 ≡ 77 mod 101
33	77 x 28 ≡ 35 mod 101
44	35 x 28 ≡ 71 mod 101
55	71 x 28 ≡ 69 mod 101
66	69 x 28 ≡ 13 mod 101
77	13 x 28 ≡ 61 mod 101
88	61 x 28 ≡ 92 mod 101
99	92 x 28 ≡ 51 mod 101
110	51 x 28 ≡ 14 mod 101

$2^{11} = 2048 \equiv 28 \pmod{101}$, so we can fill out the table by calculating powers of 28 mod 101.

Let x = 11y – z, in the equation above, so that we get:

$2^{11y-z} \equiv 6 \ (mod\ 101)$
$(2^z)2^{11y-z} \equiv (2^z)6 \ (mod\ 101)$
$2^{11y} \equiv (2^z)6 \ (mod\ 101)$

Thus, we must try different values of z, until we find $2^z(6)$ mod 101 in our answer column of our table. List these values in a table:

z	0	1	2	3	4	5	6	7	8	9
$2^z(6)$	6	12	24	48	96	91	81	61		

We can stop here because $2^{77} \equiv 61 \pmod{101}$

It follows that $2^{77} \equiv 2^7$ x 6 (mod 101) and
$2^{70} \equiv 6 \pmod{101}$, thus the solution for x is **x = 70.**

Grading: 10 pts for the table, 2 pts to take 6 and start multiplying it by powers of 2, 2 points to find 61 on the table, 1 pt for the final answer.

6) (8 pts) Use the Pollard-Rho Factoring Algorithm to determine the prime factorization of 13231. In the algorithm, at each iteration, values of a and b are determined, and then a gcd is computed. The first row of the table has been filled out for you. Please fill in each other row of the table. In order to help you, it is given that the algorithm succeeds on iteration #7. Use the space below the table for your scratch work and put the final prime factorization (2 primes) in the provided slots below.

Iteration	a	b	relevant gcd
1	5	26	1
2	26	8476	1
3	677	3418	1
4	8476	8581	1
5	11478	9279	1
6	3418	2439	1
7	12983	9970	131

All of this work is on the calculator. For each number in column a, do the following:

For example, when you have 8476, square it and add 1 to that to get 71842577. Then, mod this by 13231 to get 11478. (On a calculator, to do mod, first divide by 13231, then subtract out the integer portion of the result, then take that decimal and multiply by 13231.)

Here is the work for the gcd(13231, 12983 – 9970)

13231 = 3 x 3013 + 1179
3013 = 2 x 1179 + 655
1179 = 1 x 655 + 524
655 = 1 x 524 + 131
524 = 4 x 131

Thus,

13231 = 101 x 131

Grading: All entries were given in class except for the last two entries in column b. For this reason, the grading is as follows: 2 pts for 2439, 2 pts for 9970, 3 pts for the GCD, 1 pt for the final answer.

7) (9 pts) Consider doing a Diffie-Hellman Key Exchange with the public keys p = 31 and g = 3. Let Alice choose a private key of a = 12 and Bob choose a private key of b = 21. Calculate

(a) The value that Alice sends to Bob.
(b) The value that Bob sends to Alice.
(c) The shared key that both Alice and Bob will calculate at the end.

Please show which modular exponentiations you are calculating, and then use your calculator to compute them, just showing the result. You may break down your expressions in any way you see fit (ie. you don't have to follow exactly the fast modular exponentiation algorithm shown in class, but can use any exponential break down that makes sense to you.) Also, you may use Fermat's Theorem to get the final answer, if you deem it useful. **Note: but you do have to show clear work that indicates that you know the steps to make the calculation without a built in modular exponentiation function.**

Alice sends to Bob $3^{12} = (3^6)(3^6) = 729 \times 729 \equiv 16 \times 16 = 256 \equiv 8 \pmod{31}$

Bob sends to Alice $3^{21} = (3^{12})(3^9) \equiv 8 \times 19683 \equiv 8 \times 29 \equiv 232 \equiv 15 \pmod{31}$

Alice receives 15 from Bob and calculates $15^{12} = (15^3)^4 \equiv 3375^4 \equiv (-4)^4 \equiv 256 \equiv 8 \pmod{31}$ as their shared key.

Alice sends Bob: **8** Bob sends Alice: **15** Shared Key: **8**

Grading:

1 pt for listing 3^{12} mod 31, 2 pts for work calculating it (any reasonable breakdown is fine)

1 pt for listing 3^{21} mod 31, 2 pts for work calculating it (any reasonable breakdown is fine)

1 pt for listing either 15^{12}, 8^{21}, 3^{12*21} mod 31 for final key, 2 pts for calculation

8) (10 pts) In an RSA system, n = 493 and e = 297. What is d? (Note: Full credit will only be given to responses that appropriately use the Extended Euclidean Algorithm.)

First we must factor 493 via trial division. On the calculator, we find that 493/17 = 29. It follows that $\varphi(493) = \varphi(17) \times \varphi(29) = (17 - 1)(29 - 1) = 16 \times 28 = 448$.

It follows that $d = 297^{-1} \bmod 448$.

Let's run the Extended Euclidean Algorithm:

$448 = 1 \times 297 + 151$
$297 = 1 \times 151 + 146$
$151 = 1 \times 146 + 5$
$146 = 29 \times 5 + 1$

$146 - 29 \times 5 = 1$
$146 - 29(151 - 146) = 1$
$146 - 29 \times 151 + 29 \times 146 = 1$
$30 \times 146 - 29 \times 151 = 1$
$30(297 - 151) - 29 \times 151 = 1$
$30 \times 297 - 30 \times 151 - 29 \times 151 = 1$
$30 \times 297 - 59 \times 151 = 1$
$30 \times 297 - 59(448 - 297) = 1$
$30 \times 297 - 59 \times 448 + 59 \times 297 = 1$
$89 \times 297 - 59 \times 448 = 1$

Take this equation mod 448 to get

$89 \times 297 \equiv 1 \pmod{448}$

It follows that d = 89.

Grading: 2 pts factoring 493
1 pt phi(493)
1 pt stating that we need 297^{-1} mod 448
2 pts Euclidean
3 pts Extended Euclidean
1 pt extracting correct answer
AUTOMATIC 0/10 if they do a gcd(493,297) or gcd(492,297)

9) (10 pts) Let the public elements of an El Gamal Cryptosystem be q = 37, α = 5. Let Alice's private key $X_A = 22$. Do the following:

1. Calculate Alice's Public Key (Y_A). (Show the appropriate modular exponential breakdown.)
2. Calculate the ciphertext (C_1, C_2) when Bob sends a message to Alice where M = 9 and his randomly chosen value k = 30. In the process, show the value of K.

$Y_A = 5^{22} = (5^5)^4 5^2 = 3125^4 \times 25 \equiv 17^4 \times 25 \equiv 83521 \times 25 \equiv 12 \times 25 \equiv 300 \equiv$ **4 mod 37**

Bob calculates $K = 4^{30} = (4^{15})^2 = (2^{30})^2 \equiv 11^2 = 121 \equiv$ **10 mod 37**

Bob sends $C1 = 5^{30} = 5^{22} \times 5^8 \equiv 4 \times 390625 \equiv 4 \times 16 \equiv 64 \equiv$ **27 mod 37**

Bob sends C2 = KM = 10 x 9 = 90 ≡ **16 mod 37**

$Y_A =$ **4**, K = **10**, C1 = **27**, C2 = **16**

Grading: 1 pt expression Y_A, 2 pts simplify to 4
1 pt expression K, 1 pt simplify to 10
1 pt expression C1, 2 pts simplify to 27
1 pt expression C2, 1 pt simplify to 16
Give carry through credit if possible (so use their wrong value of K for C2 calc)

10) (10 pts) Let C be the elliptic curve $E_{31}(3, 5)$. One point on C is P = (18, 1).
What is the result of P + P? (Please provide your answer as a point.)

$$\lambda = \frac{3 \times 18^2 + 3}{2} = 975 \times 2^{-1} \equiv 14 \times 16 \equiv 224 \equiv 7 \ (mod\ 31)$$

Note that $2^{-1} \equiv 16 \bmod 31$ since 2 x 16 = 32 ≡ 1 mod 31.

Note, we can alternatively do $\frac{975}{2} \equiv \frac{14}{2} \equiv 7 \ (mod\ 31)$.

$$x_{2P} = (7^2 - 18 - 18) \equiv 49 - 36 \equiv 13 \ mod\ 31$$

$$y_{2P} = (7(18 - 13) - 1) = 35 - 1 \equiv 34 \equiv 3 \ mod\ 31$$

P + P = **(13, 3)**

Grading: 4 pts for lambda – 1 pt formula, 1 pt correct mod inverse, 2 pts answer
3 pts for x
3 pts for y, take off 1 pt if they put 34 (forgot to reduce mod 31)

11) (10 pts) Consider the task of encoding a 4-bit value (a hex character) on the Elliptic Curve $E_{79}(1, 1)$. We learned a technique in class to store an arbitrary bit string in class as a point on an Ellipitic Curve. **Using the same technique in class determine the Point encoding of the plaintext message m = 11 on the curve $E_{79}(1, 1)$.** Since this is computationally intensive, some facts will be given below that you may use to solve the problem. Use the facts as necessary. (Note: some of the facts are intentionally irrelevant, so part of what I am testing is to see if you can figure out what you actually need to use. Also, there is one calculation that I think is easy enough to do on your calculator for which I haven't provided the result.)

$11^{39} \equiv 1 \pmod{79}$
$22^{39} \equiv 1 \pmod{79}$
$27^{39} \equiv 78 \pmod{79}$
$32^{39} \equiv 1 \pmod{79}$
$43^{39} \equiv 78 \pmod{79}$
$59^{39} \equiv 78 \pmod{79}$

$11^{20} \equiv 13 \pmod{79}$
$11^{27} \equiv 52 \pmod{79}$
$27^{20} \equiv 62 \pmod{79}$
$27^{40} \equiv 52 \pmod{79}$
$40^{20} \equiv 44 \pmod{79}$
$40^{27} \equiv 67 \pmod{79}$

Step 1
In class, we stored the message in the least significant bits of the x coordinate. Thus, our message x coordinate will be of the form q x 2^4 + 11, where we try each possible value of q, starting with q = 0, until we find a value of x which has a solution for y.

We first try 0 x 2^4 + 11 = 11.
Step 1 is to compute c = 11^3 + 1 x 11 + 1 = 1331 + 12 ≡ 0 (mod 79).
Technically, in the posted code, although this value is a quadratic residue, our implementation did the following:

```
rem = pow(c, (self.p-1)//2, self.p)
if rem != 1:
    return None
```

So, for our implementation, we only consider values of x, which produce a value of c, which, when raised to the power (p-1)/2 mod p produce the value of 1. Thus, since 0 to any positive power will be 0, 11 fails.

Next, we try 1 x 2^4 + 11 = 27.
Step 1 is to compute c = 27^3 + 1 x 27 + 1 = 19711 ≡ 40 (mod 79).
Step 2 is to compute $c^{(p-1)/2}$, so 40^{39} mod 79, to see if this value is 1. Since this isn't in the chart, we can get pretty close by computing $40^{40} = (40^{20})^2 \equiv 44^2 \equiv 1936 \equiv 40 \pmod{79}$. It follows since $40^{40} = 40^{39}$ x 40 ≡ 40 (mod 79), that we can multiply this equation through by 40^{-1} to prove that $40^{39} \equiv 1 \pmod{79}$. This means that we have a matching value of y!!!
Step 3 is to compute the matching value of y. The matching y value must be $40^{(79+1)/4} = 40^{20}$ mod 79. Look this up on the chart to find that the matching y value is 44.

Plaintext Point = **(27, 44)**

Grading: 3 pts to obtain the correct x value of 27.
3 pts to plug in 27 into the curve equation to get 40.
3 pts to take 40 and exponentiate it to the right value to get 44.
1 pt to correctly fill in the point.
Note: I decided to accept (11, 0) even though it's not the point produced by my code.