Midterm 1
Math 116, Spring 2021

Name:	**UID:**

Honor Statement
I assert, on my honor, that I have not received assistance of any kind from any other people, including posting exam questions on online forums while working on this Final Exam. I have only used non-human resources, for example Internet, calculators, textbook, notes, and lecture videos, during the period of this evaluation.

Signature: _____

Directions—Please read carefully!

- You have a 24-hour window

  April 21 (Wed) 8am PDT – April 22 (Thurs) 8am PDT

  to complete the exam, but the exam is designed to be able to be finished in 1 hour.
- On April 21 (Wed) 9–9:50am PDT, I will be on Zoom for any questions about statements of exam problems. You can also use Piazza to ask, but please use private message to avoid leaking your solution to others.
- You are allowed to use any non-human resources including internet, calculators, textbook, notes, lecture videos, etc. **You are NOT allowed to seek help from other people, including posting exam questions on online forums.**
- In order to receive full credit, you must **show your work or explain your reasoning**; your final answer is less important than the reasoning you used to reach it. Correct answers without work will receive little or no credit. Please write neatly. **Illegible answers will be assumed to be incorrect.** Circle or box your final answer when relevant.
- The exam is on Gradescope. Please either
  - Write your answers on the pdf file of the exam, then submit onto Gradescope,
  - Print the exam and write your answers on the exam paper, then scan and submit onto Gradescope, or
  - Use blank sheets of paper, **copy the honor statement and sign.** Then write your answers on them, scan and submit onto Gradescope.

Good luck!

1. You do NOT need to provide explanation to the following questions.

(5) (a) Which of the following is an asymmetric cipher? Select ALL which are correct.

A. Hill Cipher
B. Substitution Cipher
C. Shift Cipher
✓ D. Elgamal
✓ E. Diffie–Hellman key exchange

(3) (b) Affine Cipher is intrinsically vulnerable to which of the following attack? Select All which are correct.

A. Brute-force attack
✓ B. Known plaintext attack
✓ C. Chosen plaintext attack

(5) (c) Which of the following is a polynomial time algorithm? Select All which are correct.

✓ A. Euclidean Algorithm
B. Brute-force algorithm to solve Discrete Log Problem
C. Shank's Babystep–Giantstep Algorithm
D. Pohlig–Hellman Algorithm
✓ E. Fast Powering Algorithm

The problem (d) has a mistake because 2 is in fact not a generator. However, the problem is only asking the general method to check whether an element is a generator, so should not affect your answer much.

(6) (d) To prove that 2 is a generator/primitive root of $(\mathbb{Z}/71\mathbb{Z})^\times$, we know it is sufficient to verify that $2^a \neq 1$, $2^b \neq 1$ and $2^c \neq 1$. If $1 < a < b < c < 71$, then

$a =$ 10, $b =$ 14, $c =$ 35.

$70 = 2 \cdot 5 \cdot 7$

$a = \frac{70}{7} = 10, \quad b = \frac{70}{5} = 14, \quad c = \frac{70}{2} = 35$

(10) 2. (a) What is the order of the multiplicative group $(\mathbb{Z}/35\mathbb{Z})^\times$.

$35 = 5 \cdot 7$

$|(\mathbb{Z}/35\mathbb{Z})^\times| = \phi(35) = (5-1)\cdot(7-1) = 24$

(13) (b) Find the order of the element 2 in $(\mathbb{Z}/35\mathbb{Z})^\times$.

- $24 = 2^3 \cdot 3$

  $2^{\frac{24}{2}} = 2^{12} = 2^5 \cdot 2^5 \cdot 2^2 = 32 \cdot 32 \cdot 4 \equiv (-3)\cdot(-3)\cdot 4$

  $\equiv 1 \pmod{35}$

- $12 = 2^2 \cdot 3$

  $2^{\frac{12}{2}} = 2^6 = 64 \equiv -6 \pmod{35}$

  $2^{\frac{12}{3}} = 2^4 = 16 \pmod{35}$

$\Rightarrow \operatorname{ord}(2) = 12$

(15) 3. Find integers u, v such that $71u + 23v = 1$, and u is positive and smallest possible.

Extended Euclidean Algorithm

3	71	23	11
	69	22	
	2	1	

	u	v	q
71	1	0	
23	0	1	
2	1	-3	3
1	-11	34	11

$71 \cdot (-11) + 23 \cdot 34 = 1$

$\Rightarrow 71 \cdot (-11+23) + 23 \cdot (34-71) = 1$

i.e. $71 \cdot 12 + 23 \cdot (-37) = 1$

$\boxed{u = 12, \quad v = -37}$

(13) 4. Find all solutions $x \in \mathbb{Z}$ such that $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4$, and $x \equiv 3 \pmod 5$.

- $x_1 \equiv 2 \pmod 3$
- $x_2 \equiv 2 + 3 \cdot y_2 \pmod{3 \cdot 4}$

  $\equiv 1 \pmod 4$

  $\Rightarrow y_2 \equiv (-1) \cdot 3^{-1} \equiv 1 \pmod 4$

  $x_2 \equiv 5 \pmod{12}$
- $x_3 \equiv 5 + 12 \cdot y_3 \pmod{12 \cdot 5}$

  $\equiv 3 \pmod 5$

  $\Rightarrow y_3 \equiv (-2) \cdot 12^{-1} \equiv (-2) \cdot 3 \equiv 4 \pmod 5$

  $\Rightarrow x_3 \equiv 5 + 12 \cdot 4 \equiv 53 \pmod{60}$

Conclusion: All $x \in \mathbb{Z}$ s.t. $x \equiv 53 \pmod{60}$ is a solution

(15) 5. Bob is using Elgamal PKC to send a secret message to Alice. They use $\mathbb{F}_{29}^{\times}$ with generator $g = 2$. They also agree to match $1, 2, 3, ..., 28 \in \mathbb{F}_{29}^{\times}$ with symbols a,b,c,...,z, comma, period. Alice received two pieces of ciphertexts from Bob: $(c_1, c_2) = (6, 13)$ and $(c_1, c_2) = (6, 2)$. Knowing Alice's private key is 5, please help Alice decrypt Bob's two-symbol message.

Let $a = 5 \in \mathbb{F}_{29}^{\times}$ be the private key

$m = c_2 \cdot c_1^{-a}$ is the plaintext

- $c_1^{-a} = 6^{-5} \equiv 5^5 \equiv 25 \cdot 25 \cdot 5 \equiv (-4) \cdot (-4) \cdot 5$

  $\equiv (-4) \cdot 9 \equiv -7 \pmod{29}$

- $m = c_2 \cdot c_1^{-a} \equiv 13 \cdot (-7) \equiv -91 \equiv 25 \pmod{29}$

- $m = c_2 \cdot c_1^{-a} \equiv 2 \cdot (-7) \equiv 15 \pmod{29}$

$25 \leftrightarrow$ Y

$15 \leftrightarrow$ O

message = YO

(15) 6. It is known that 2 is a generator of $\mathbb{F}_{19}^{\times}$. Use Shank's Babystep-Giantstep algorithm to find $x \in \mathbb{Z}/18\mathbb{Z}$ such that $2^x \equiv 5 \pmod{19}$. (Hint: Modulo 19, the inverse of 13 is 3.)

$N = \text{ord}(2) = 18$

$n = \lfloor \sqrt{N} \rfloor + 1 = 5$

List 1:	g^0	g^1	g^2	g^3	g^4	g^5, g^{-5}
	1	2	4	8	16	$32 \equiv 13$ 3

List 2:	h	$h \cdot g^{-5}$	$h \cdot g^{-10}$	$h \cdot g^{-15}$	$h \cdot g^{-20}$
	5	$5 \cdot 3$	45	21	
		15	7	2	

$h \cdot g^{-15} = g^1 \Rightarrow h = g^{16} \Rightarrow \boxed{x = 16}$

Check: $2^{16} \equiv 2^{-2} \equiv 4^{-1} \equiv 5 \pmod{19}$