Comment (2024): this exam is from an older version of this course, taught at Brown. There are some differences of style and emphasis compared to Math 252 here. I've updated the notation in this file to notation we use in our course, but you may see some different notation in the solutions, since I used slightly different notation in this course.

1. Alice and Bob are using Elgamal encryption, with public parameters $p = 29, g = 19$. The summary table for Elgamal is on the back page of this packet. There is also a multiplication table for $\mathbb{Z}/29\mathbb{Z}$, so that you do not need to do the arithmetic by hand.

   (a) [3 points] Alice chooses the private key $a = 9$. What is her public key? Express your answer as an integer in $\{0, 1, 2, \cdots, 28\}$.

   (b) [3 points] Bob sends ciphertext $(8, 25)$ to Alice. What is the plaintext? Express your answer as an integer in $\{0, 1, 2, \cdots, 28\}$.

2. (a) [3 points] Suppose that $a \mid m$. Prove that the congruence $ax \equiv ab \pmod{m}$ holds if and only if the congruence $x \equiv b \pmod{\frac{m}{a}}$ holds (all variables are integers).

   (b) [3 points] Suppose that $\gcd(a, m) = 1$. Prove that the congruence $ax \equiv ab \pmod{m}$ holds if and only if the congruence $x \equiv b \pmod{m}$ holds.

3. [6 points] Write a program that reduces breaking Diffie-Hellman key exchange to breaking Elgamal encryption.

   More precisely: suppose that Eve has written a function `break_elg(p,g,A,c1,c2)` with the following behavior: if the arguments are as in Table 2.3 (back of the packet), then this function will return m. Make use of this function to write a function `break_dh(p,g,A,B)`, which accepts arguments as labeled in Table 2.2 and returns the corresponding shared secret.

   You may use any functions that are built into Python (or any language you have written your homework in), plus the hypothetical function `break_elg`. You may also assume that you have already written a function `ext_euclid(a,b)`, with the following behavior: given two positive integers a, b, this function returns a list of three integers $[u, v, d]$, where $d = \gcd(a, b)$ and $au + bv = d$.

   For full points, your program must require at most $\mathcal{O}(\log p)$ arithmetic operations (not counting any operations needed to compute `break_elg`).

4. Let p be a prime number, and g an element of $(\mathbb{Z}/p\mathbb{Z})^\times$.

   (a) [3 points] Prove that if $\operatorname{ord}_p g = 17$, then $p \equiv 1 \pmod{17}$.

   (b) [3 points] Prove conversely that if $p \equiv 1 \pmod{17}$, then there exists some element $[g]_p$ of order 17.

5. [6 points] Suppose that Alice and Bob use the following variant of Elgamal. The parameters p, g are as in table 2.3, and Alice chooses a secret key a and public key A in the same manner as in table 2.3. However, instead of following table 2.3, Bob computes his ciphertext as follows: he chooses a random element k, and computes

$$
\begin{aligned}
c_1 &\equiv A^k \pmod{p} \\
c_2 &\equiv m \cdot g^k \pmod{p},
\end{aligned}
$$

then sends (c_1, c_2) to Alice.

Explain how Alice can efficiently decipher messages, i.e. determine m from (c_1, c_2). You will need to place a restriction on Alice's original choice of private key a in order for decryption to be possible; clearly state this restriction.

Reference information. You may detach this sheet for easier use.

Public parameter creation	
A trusted party chooses and publishes a (large) prime p and an integer g having large prime order in $\mathbb{F}_p^*$.	
Private computations	
Alice	**Bob**
Choose a secret integer a.	Choose a secret integer b.
Compute $A \equiv g^a \pmod{p}$.	Compute $B \equiv g^b \pmod{p}$.
Public exchange of values	
Alice sends A to Bob $\longrightarrow$ A	
B $\longleftarrow$ Bob sends B to Alice	
Further private computations	
Alice	**Bob**
Compute the number $B^a \pmod{p}$.	Compute the number $A^b \pmod{p}$.
The shared secret value is $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod{p}$.	

Table 2.2: Diffie–Hellman key exchange

Public parameter creation	
A trusted party chooses and publishes a large prime p and an element g modulo p of large (prime) order.	
Alice	**Bob**
Key creation	
Choose private key $1 \le a \le p-1$. Compute $A = g^a \pmod{p}$. Publish the public key A.	
Encryption	
	Choose plaintext m. Choose random element k. Use Alice's public key A to compute $c_1 = g^k \pmod{p}$ and $c_2 = mA^k \pmod{p}$. Send ciphertext (c_1, c_2) to Alice.
Decryption	
Compute $(c_1^a)^{-1} \cdot c_2 \pmod{p}$. This quantity is equal to m.	

Table 2.3: Elgamal key creation, encryption, and decryption

Multiplication table modulo 29

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
2	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	1	3	5	7	9	11	13	15	17	19	21	23	25	27
3	0	3	6	9	12	15	18	21	24	27	1	4	7	10	13	16	19	22	25	28	2	5	8	11	14	17	20	23	26
4	0	4	8	12	16	20	24	28	3	7	11	15	19	23	27	2	6	10	14	18	22	26	1	5	9	13	17	21	25
5	0	5	10	15	20	25	1	6	11	16	21	26	2	7	12	17	22	27	3	8	13	18	23	28	4	9	14	19	24
6	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23
7	0	7	14	21	28	6	13	20	27	5	12	19	26	4	11	18	25	3	10	17	24	2	9	16	23	1	8	15	22
8	0	8	16	24	3	11	19	27	6	14	22	1	9	17	25	4	12	20	28	7	15	23	2	10	18	26	5	13	21
9	0	9	18	27	7	16	25	5	14	23	3	12	21	1	10	19	28	8	17	26	6	15	24	4	13	22	2	11	20
10	0	10	20	1	11	21	2	12	22	3	13	23	4	14	24	5	15	25	6	16	26	7	17	27	8	18	28	9	19
11	0	11	22	4	15	26	8	19	1	12	23	5	16	27	9	20	2	13	24	6	17	28	10	21	3	14	25	7	18
12	0	12	24	7	19	2	14	26	9	21	4	16	28	11	23	6	18	1	13	25	8	20	3	15	27	10	22	5	17
13	0	13	26	10	23	7	20	4	17	1	14	27	11	24	8	21	5	18	2	15	28	12	25	9	22	6	19	3	16
14	0	14	28	13	27	12	26	11	25	10	24	9	23	8	22	7	21	6	20	5	19	4	18	3	17	2	16	1	15
15	0	15	1	16	2	17	3	18	4	19	5	20	6	21	7	22	8	23	9	24	10	25	11	26	12	27	13	28	14
16	0	16	3	19	6	22	9	25	12	28	15	2	18	5	21	8	24	11	27	14	1	17	4	20	7	23	10	26	13
17	0	17	5	22	10	27	15	3	20	8	25	13	1	18	6	23	11	28	16	4	21	9	26	14	2	19	7	24	12
18	0	18	7	25	14	3	21	10	28	17	6	24	13	2	20	9	27	16	5	23	12	1	19	8	26	15	4	22	11
19	0	19	9	28	18	8	27	17	7	26	16	6	25	15	5	24	14	4	23	13	3	22	12	2	21	11	1	20	10
20	0	20	11	2	22	13	4	24	15	6	26	17	8	28	19	10	1	21	12	3	23	14	5	25	16	7	27	18	9
21	0	21	13	5	26	18	10	2	23	15	7	28	20	12	4	25	17	9	1	22	14	6	27	19	11	3	24	16	8
22	0	22	15	8	1	23	16	9	2	24	17	10	3	25	18	11	4	26	19	12	5	27	20	13	6	28	21	14	7
23	0	23	17	11	5	28	22	16	10	4	27	21	15	9	3	26	20	14	8	2	25	19	13	7	1	24	18	12	6
24	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5
25	0	25	21	17	13	9	5	1	26	22	18	14	10	6	2	27	23	19	15	11	7	3	28	24	20	16	12	8	4
26	0	26	23	20	17	14	11	8	5	2	28	25	22	19	16	13	10	7	4	1	27	24	21	18	15	12	9	6	3
27	0	27	25	23	21	19	17	15	13	11	9	7	5	3	1	28	26	24	22	20	18	16	14	12	10	8	6	4	2
28	0	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1