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. [10 points] (a) Find integers u, v such that $91u + 74v = 1$.

   (b) Find an integer x such that $74x \equiv 5 \pmod{91}$.

2. [10 points] Alice and Bob are performing Diffie-Hellman key exchange using the following parameters.

$$\begin{aligned} p &= 19 \\ g &= 2 \end{aligned}$$

   (a) Alice chooses the secret number $a = 3$. What number does she send to Bob?

   (b) Bob sends Alice the number $B = 4$. What is Alice and Bob's shared secret?

3. [10 points] Alice and Bob are using the ElGamal cryptosystem, with the following parameters.

$$\begin{aligned} p &= 13 \\ g &= 7 \end{aligned}$$

   (a) Alice chooses the private key $a = 2$. What is her public key, A?

   (b) Suppose that Alice receives the ciphertext $(c_1, c_2) = (2, 6)$ from Bob. What is the corresponding plaintext?

4. [10 points] Suppose that p is a prime number at most n bits in length, and a is an element of $(\mathbf{Z}/p\mathbb{Z})^\times$. Write a function `inverse(a,p)` which takes the integers a, p as arguments and returns the inverse of a modulo p. For full points, your function should perform at most $\mathcal{O}(n)$ arithmetic operations, and the return value should be an integer between 1 and $p-1$ inclusive.

5. [10 points] (a) Let p be a prime, and $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Define the *order of a modulo p*.

   (b) Let $p = 2^{16} + 1$ (this number is known to be prime). Prove that for any $a \in (\mathbf{Z}/p\mathbb{Z})^\times$ except 1, $\mathrm{ord}_p(a)$ is even. You may use any facts proved in the class or on the homework.

   (c) Suppose that $p = 2^{16} + 1$, as in the previous part. What is $\mathrm{ord}_p(2)$?

   (d) Suppose that p is a prime with the property that $\mathrm{ord}_p(a)$ is even for every $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ except 1. Prove that $p = 2^n + 1$ for some integer n. You may use any facts proved in the class or on the homework.

6. [10 points] Alice and Bob have chosen parameters p, g (p is a prime, $g \in (\mathbf{Z}/p\mathbb{Z})^\times$) for Diffie-Hellman key exchange.

   On Monday, Alice sends Bob the number A, Bob sends Alice the number B, and they establish a shared secret S.

   On Tuesday, Alice sends Bob the number A', Bob sends Alice the number B', and they establish a shared secret S'.

Eve intercepts A, B, A', and B' (as usual), and she also manages to steal the first shared secret S from a post-it note in Bob's trash Monday night. Suppose that she also discovers the following two facts (possibly resulting from lazy random number generation by Alice and Bob).

$$\begin{aligned} A' &\equiv g^2 A \pmod{p} \\ B' &\equiv B^2 \pmod{p} \end{aligned}$$

How can Eve can use this information to efficiently compute the second shared secret S'?