Instructions:

Homework should be done in groups of one to three people. You are free to change group members at any time throughout the quarter. Problems should be solved together, not divided up between partners. In your submission, you must indicate the name of each partner within your group. Each member of your group must submit his/her own work through Gradescope. Submissions must be received by 10:00pm on the due date, and there is no exception to this rule.

You will be able to look at your scanned work before submitting it. Please ensure that your submission is legible (neatly written and not too faint) or your homework may not be graded.

Students should consult their textbook, class notes, lecture slides, instructor, and TA’s when they need help with homework. Students should not look for answers to homework problems in other texts or sources, including the Internet. You may ask questions about the homework in office hours and on Piazza. However, you should only use Piazza to ask for clarifications on the homework problems. Publicly posting any part of your work on Piazza will be considered cheating, and the author of the post will receive a zero on the entire assignment!

Your assignments in this class will be evaluated not only on the correctness of your answers, but on your ability to present your ideas clearly and logically. You should always explain how you arrived at your conclusions and justify your answers with mathematically sound reasoning. Whether you use formal proof techniques or write a more informal argument for why something is true, your answers should always be well-supported. Your goal should be to convince the reader that your results and methods are sound.

1. a. Compute the appropriate cyclotomic polynomial and use it to decide which of 5 and/or 7 is a primitive root mod 37.
   b. Compute the appropriate cyclotomic polynomial and use it to find all primitive roots modulo 19.

2. Alice and Bob use Diffie-Hellman key exchange protocol to communicate in secret. They publicly announce a prime number \( p = 23 \) and a primitive root \( r = 5 \) under modulus 23. Alice picks a secret key \( a = 6 \) and in turn receive the key \( \beta = 19 \) from Bob.
   a. What is the key that Alice sends to Bob?
   b. What is the shared secret key?
   c. Can Alice compute Bob’s private key using only what she’s given?

3. This time, Alice and Bob use El Gamal protocol to communicate in secret. They publicly announce a prime \( p = 139 \) and a primitive root \( r = 3 \). Bob chooses a private key \( b = 12 \). To send a message \( M = 100 \), Alice chooses the session key \( k = 52 \) and sends to Bob two number \( (U, V) \).
   a. What is Bob’s public key?
   b. Compute \((U, V)\).
   c. How will Bob recover Alice’s message?

4. Consider the elliptic curve \( E : y^2 = x^3 - 15x + 18 \).
   a. Check that it is a valid elliptic curve.
   b. Check that the point \( P = (1, 2) \) is on the curve.
   c. Let \( P' = (1, -2) \). Compute \( P + P' \).
   d. Compute \(-P\) and \(2P\).
   e. Check that the point \( Q = (7, 16) \) is on the curve.
   f. Compute \(-Q\) and \(P + Q\).

5. Alice and Bob agree to use the elliptic curve \( E : y^2 = x^3 + 3x + 17 \) mod the prime \( p = 47 \) and the point \( P = (5, 4) \) for a Diffie-Hellman public key exchange. Alice chooses the secret exponent \( N_A = 3 \) and Bob chooses the secret exponent \( N_B = 5 \).
   a. Check that this is a valid curve and the point \( P \) is on the curve.
   b. Compute Alice’s public key \( Q_A = N_A P \).
   c. Compute Bob’s public key \( Q_B = N_B P \).
   d. What is their shared secret key?
   e. Alice knows the curve \( E \), the prime \( p \), the point \( P \) on the curve, her own secret and public keys \( N_A, Q_A \) and Bobs public key \( Q_B \). Can she recover Bob’s secret exponent \( N_B \)? Justify your answer.