Computations:

1. A. Use the Euclidean algorithm to find \( g = \gcd(67, 54) \).
   
   B. Find integers \( x \) and \( y \) so that \( 67x + 54y = g \).
   
   C. Find a number \( z \) between 0 and 66 so that \( 54z \equiv 1 \mod 67 \).

2. How many affine ciphers are there for an alphabet of 9900 letters?

3. What is the period of a Vigenere cipher in which you encrypt a message first with a Vigenere cipher of period 6 and then encrypt the ciphertext with a Vigenere cipher of period 9?

4. Find an integer \( x \) between 0 and 72 so that \( x \equiv 3^{734} \mod 73 \).

5. Find an integer \( x \) so that \( x \equiv 1 \mod 4 \) and \( x \equiv 2 \mod 5 \). Then find another one.

Short-answer questions: (1-2 sentences only).

1. Why is it possible to decode a message encrypted with the affine cipher if you know the first two letters of the plaintext?

2. How are dot products useful for breaking the Vigenere cipher?

3. Explain why there are gaps of arbitrarily long length between primes.

4. What are some of Euler’s contributions to number theory?

5. How do you encode and decode with the RSA cryptosystem?

Bonus:

Suppose \( p \) is a prime number and \( a \) and \( b \) are integers.

Prove that if \( p \) divides \( ab \) then \( p \) divides \( a \) or \( p \) divides \( b \).

Use this to show that if \( x^2 \equiv 1 \mod p \) then \( x \equiv \pm1 \mod p \).

Give a specific example to show the last sentence can be false if \( p \) is not prime.