CS5285: Information Security for eCommerce Autumn, 2024
Tutorial 4, Week 5 (Oct 8)

Questions:

1. **Modular Exponentiation**

   (a) Calculate $17^{27} \mod 23$.

   (b) Consider the following two cases of raising a number to a certain exponent:

   - $a^{255} \mod b$
   - $a^{257} \mod b$

   Using the square and multiply method, which one of these two exponentiations will be significantly more expensive? Why? Calculate the total number of modular multiplications required for each case (counting a squaring operation as a modular multiplication).

2. **Modular Inverse**:

   (a) Calculate the modular inverse of 2019 mod 5285 (Use the extended Euclidean Algorithm).

   (b) Without calculating anything, can you tell whether 360 mod 555 has a modular inverse? Explain why.

3. **Eulers Totient**

   1) Calculate $\phi(n)$ for the following values of n.

   (a) $n = 83$

   (b) $n = 1210$

   2) Calculate $39^{191} \mod 47$

4. **RSA Encryption** Suppose we are using an RSA encryption scheme with $n = pq$, private key d, public key e, where the ciphertext is calculated as $C = M^e \mod n$ and can be decrypted by checking $C^d \mod n = M$.

   (a) Can you show why RSA encryption works? Hint: Fermat's Little Theorem...

   (b) Can you encrypt M when it is larger than n?