COMP 2711 Discrete Mathematical Tools for Computer Science
2022 Fall Semester – Tutorial 9

Question 1: Evaluate $1819^{13} \pmod{2537}$). Show the steps of fast modular exponentiation.

Question 2: Compute each of the following. Show or explain your work. Do not use a calculator or computer.

1) 15^{96} mod 97.
2) 67^{72} mod 73.
3) 67^{73} mod 73.

Question 3: (a) Use Fermat's Little Theorem to show that, if an integer a is not divisible by any of 3, 5, and 7, then

$$a^{49} \equiv a \pmod{105}.$$

(b) Use part (a) to calculate

$$4^{385} \bmod 105.$$

Question 4: This problem is on the RSA algorithm for public key cryptography. To generate his keys, Bob starts by picking $p = 37$ and $q = 31$. So, $n = pq = 1147$ and $T = (p-1)(q-1) = 1080$.

(a) Bob's public key is a pair $(e, 1147)$. Which of the following integers can Bob use for e? Why?

(i) 17; (ii) 5; (iii) 49; (iv) 21.

(b) Suppose Bob chooses $e = 47$. Compute his private key d by running the extended GCD algorithm. Show all the steps.

Question 5: Consider the following simplified version of the RSA algorithm for public cryptography:

(i) Bob's public key is a pair (n, e), where n is a prime number and e is a positive integer that is smaller than n and is relatively prime with $n - 1$.

(ii) Bob's private key is $d = e^{-1} \bmod (n-1)$.

(iii) Alice encrypts a message m $(0 < m < n-1)$ by calculating $c = m^e \bmod n$, and sends the ciphertext c to Bob.

(iv) Bob decrypts the ciphertext c by calculating $c^d \bmod n$.

Suppose $n = 251$ and $e = 137$.

(a) Calculate d using the extended GCD algorithm. Show the computational steps.

(b) Suppose $m = 200$. Calculate $c = m^e \bmod n$ using repeated squaring. Show the computational steps.

(c) Is the system secure? Explain why or why not.