Network Security Technology

Tutorial 4, Week 4 (March 16)

Due Date: March 23

Spring, 2021 LIU Zhen

Questions:

- 1. Determine whether 227 and 79 are relatively prime. (10 points)
- 2. Find the multiplicative inverse of 79 mod 229. (10 points)
- 3. Without calculating anything, by simply looking at the numbers, can you tell whether 7932 has a multiplicative inverse mod 11958? Explain your solution. (10 points)
- 4. Show the steps of how to calculate $\phi(315)$. (20 points)
- 5. Calculate $227^{54996213} \mod 21$ as efficient as possible. (20 points)
- 6. Determine whether the following groups are cyclic. If they are, give a generator of the group. (30 points)
 - $(Z_5, +)$ (i.e., the set of numbers modulo 5 with addition as the group operation)
 - (Z_8^*, \times)