Network Security Technology Spring, 2019
Tutorial 2, Week 3 (March 13) LIU Zhen
Due Date: March 20

Questions:

1. **Euclidean Algorithm (15 points)**:
   (a) Determine whether 227 and 79 are relatively prime.
   (b) Determine whether 22337 and 17241 are relatively prime.
2. **Extended Euclidean Algorithm (15 points)**:
   (a) Find the multiplicative inverse of $4565 \mod 15447$.
   (b) Without calculating anything, by simply looking at the numbers, can you tell whether $7932 \mod 11458$ has a multiplicative inverse? Explain.
3. **Euler Phi Function (10 points)**:
   (a) Show the steps of how to calculate $\phi(210)$.
4. **Fermat's Little Theorem/Euler's Generalization (15 points)**:
   (a) Show how to calculate $227^{54996213} \mod 21$ using Euler's generalization.
5. **Modular Exponentiation (20 points)**
   (a) Calculate $17^{27} \mod 23$ using the square and multiply method.
   (b) Consider the following two cases of raising a number to a certain exponent:
      - $a^{65535} \mod b$
      - $a^{65537} \mod b$

      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).
6. **Group (10 points)**
   (a) Which of the following sets form a multiplicative group? How can you tell?
      - $\mathbb{Z}_{11} \setminus \{0\}$
      - $\mathbb{Z}_{15} \setminus \{0\}$
      - $\mathbb{Z}_{69} \setminus \{0\}$
      - $\mathbb{Z}_{79} \setminus \{0\}$
7. **Cyclic Group (15 points)** Determine whether the following groups are cyclic. If they are, give a generator of the group.
   - $(\mathbb{Z}_5, +)$ (i.e., the set of numbers modulo 5 with addition as the group operation)
   - $(\mathbb{Z}_8^*, *)$
   - $(\mathbb{Z}_{13}^*, *)$