ECE4802/CS4801 Assignment #4

Deadline: Dec 5, 11:59pm.

Show your work and intermediate steps of the computations for each question.

1. Consider the multiplicative group of $\mathbb{Z}_{79}^*$.
   a. What are the possible element order? How many element exist for each order ?
   b. Determine the order of all elements of $\mathbb{Z}_{79}^*$.
   c. What are the generators of $\mathbb{Z}_{79}^*$?
   d. Write the elements of $\mathbb{Z}_{79}^*$ as powers of 7.

2. Use Baby-step Giant-step Algorithm to compute following discrete logarithm problems:
   a. $15 = 2^x \ mod\ 59$ ($or\ equivalently\ \log_2 15\ mod\ 59$)
   b. $23 = 11^x \ mod\ 79$ ($or\ equivalently\ \log_{11} 23\ mod\ 79$)
   c. $7 = 11^x \ mod\ 79$ ($or\ equivalently\ \log_{11} 7\ mod\ 79$)
   d. $100 = 7^x \ mod\ 103$ ($or\ equivalently\ \log_7 100\ mod\ 103$)
   e. $100 = 7^x \ mod\ 101$ ($or\ equivalently\ \log_7 100\ mod\ 101$)

3. D-H Key Exchange: Alice and Bob want to generate a common key. They agreed to use prime number $p = 809$ and generator $\alpha = 3$. Alice's private key= 17, Bob's private key= 41.
   Find the the followings and show every intermediate step:
   a. Alice's public key
   b. Bob's public key
   c. Common key generated by Alice and Bob