Cryptography and Network Security I
HW 2 Programming Part a.
Due October 11, 2018

In class we discussed replay attacks, authentication, and session key distribution. The Needham–Schroeder Symmetric Key Protocol, based on a symmetric encryption algorithm was one of them. We also studied the shared key generation without a third trusted party and learned DIffie-Hellman key exchange algorithm.

In this assignment

1. You are asked to implement N-S protocol and ensure that it is safe against to replay attacks. Explain your implementation details in a README file.

2. To establish initial shared keys between Alice and the Key Distribution Center (KDC), and Bob and KDC use Computational DIffie-Hellman key exchange protocol. Explain your assumptions, set up, and algebraic constructions in a README file.

Note: your write up can be up to 5 pages long with double space 12 pnt font.