CS 5490/6490: Network Security – Fall 2015  
Homework 4  
Due by 1:25 PM MT on Wednesday November 11th 2015

Important:  
• No cheating will be tolerated  
• NO EXTENSIONS

Total points for this homework:  cs5490 = 34  cs6490 = 42

Question 1 (Session Keys) (2 points): Chapter 11, problem 3.

Question 2 (Lamport’s Hash and Strong Password Protocols):  
(a) (3 points) Chapter 12, problem 5.  
(b) (3 points) Chapter 12, problem 14.  
(c) (3 points) Chapter 12, problem 15.

Question 3 (Real-Time Security):  
(a) (7 points) Chapter 16, problem 1 (each part – 1 point).  
(b) (3 points) Chapter 16, problem 5.  
(c) (3 points) Chapter 16, problem 6.  
(d) (2 points) Chapter 16, problem 12.

Question 4 (IPsec):  
(a) (3 points) Is it possible to use encapsulate an AH packet within an ESP packet and vice versa? Explain with the help of examples.  
(b) (2 points) Chapter 17, problem 1.  
(c) (3 points) Chapter 17, problem 7.

Answer the following questions (in your own words, do not copy text) based on this paper.  
1. What are the advantages of building security at the TCP layer?  
2. Explain the role of Self-spreading Transport (STP) in 3-4 sentences.  
3. How does TCPsec interoperate with NATs?  
4. Why does TCPsec handshake perform better than SSL?