Assignment 3—Chapter 2
CptS 427/527—Network Security
Assigned: 20 February 2008
Due: 27 January 2008, 4:15 pm

Explain and/or justify all of your answers. Short answers are sufficient, but ‘Yes’/’No’ answers will not receive full credit. If you make any assumptions, please state them.

Chapter 2
Answer the following questions from the Exercises (pgs 94-97).
10 Pts  Question 2.1
10 Pts  Question 2.4
10 Pts  Question 2.16
10 Pts  Question 2.17
15 Pts  Question 2.20
10 Pts  Question 2.22
10 Pts  Question 2.25
10 Pts  Question 2.33
10 Pts  Question 2.34

Answer the following two questions.
10 Pts  Define the acronyms ECB, CBC, and CTR. Name at least two advantages that CBC and CTR have over ECB.
10 Pts  What two design criteria of AES make it significantly strong than DES, its predecessor. Explain the impact of these two design choices.