CS 795 November 16, 2016

Homework 4

Students are welcome to work together, but *every student must write up their own solutions, independently!* I strongly encourage students to use LaTex for writing up their solutions. Please see the course web-page for a template file.

Each question is worth 10 points.

Question 1: Exercise 8.1 in the book

Question 2: Exercise 8.5 in the book
(Hint: note the group operation before jumping to an answer!)

Question 3: Exercise 8.9 in the book

Question 4: Exercise 8.7 in the book

Question 5: Exercise 8.14 in the book.
(I find the wording a bit confusing. It should read: "Show that it is possible to construct an adversary A' for which $\Pr[A'([x^e \bmod N]) = x] = 0.99]$ for *all* $x \in \mathbb{Z}_N^*$".)