Practice questions for take home final

Boaz Barak

Here are some questions that would serve as good preparation for the final exam:

From my Princeton course finals:

Spring 2010: Question 1 (except for one way functions, which we didn't learn about), Question 2, Question 3, Question 4

Fall 2007: Question 2, Question 3, Question 4

Fall 2005: Question 1, Question 2, Question 3

Dan Boneh's Stanford CS255: Cryptography and computer security (finals at the bottom of page)

Winter 2016 final: Problem 1b,1c, Problem 2 (the key here is the pair of string k_0, k_1, PRP stands for pseudorandom permutation) a-c - you can also prove that if *pi* is a *random permutation* then this is in fact a PRP, Problem 3 - we talked about the Davies-Meyer construction of a hash function from a block cipher and it is also described in the question. Problem 4- the notion of "semantically secure" here is that encryption of 0 is indistinguishable from encryption of 1 (this is not the same as CPA since this is a private key encryption), Problem 5, Problem 6

Winter 2015 final: Problem 1a,b,c,d,e . Problem 2, Problem 3a-c, Problem 4, Problem 5.

Prior years' finals might also be useful. In addition questions from both the Katz-Lindell textbook as well as the Boneh-Shoup text can be useful resources.