Mathematical Cryptology 2013

Dept. of EIT
Lund University
Box 118, 221 00 Lund, Sweden

WEEK 6,

Reading instructions:

- Chapter 19 (last part)
- Chapter 20

There will be 2 hours of lectures covering the above.

Hand-in exercises:

1) Review exercises: 20

2) Standard exercises: 19

3) Programming exercise: -

Hand in no later than before the exam.

Ch 20: Review exercises:

20.1 What is the random oracle model and why does a proof in the random oracle model not apply to the real world.
20.2 What is the forking lemma?
20.3 How does RSA-OAEP work?

Ch 19: Standard exercises:
19.4 Show that in our definition of $\mathcal{BPP}$ one can replace the constant 2/3 by any proportion in the range $(1/2, 1)$. 19.5 Show that if one-way functions exist then $\mathcal{P} \neq \mathcal{NP}$.

EXAM: Friday March 5, 8.00-13.00 at the department (exact location later)
Both programming exercises must have be approved before the exam! The exam will be review exercises (40%) and problem solving exercises (60%). Not the same as your hand-in exercises, but similar. See the course webpage, where you find old exams.

The book is not allowed on the exam, but complicated formulas will be given on the exam if they are needed. Do not forget to bring a good calculator.