Take-Home Exam

The following exercises are from (Katz & Lindell, 2014).

- Instead of final exam question(s) on “Authenticated Encryption”, you can solve:
  - Exercise 4.25, page 150.

- Instead of final exam question(s) on “Hash Functions”, you can solve all of the following:
  - Exercise 5.2, page 190.
  - Exercise 5.6, page 190.
  - Exercise 5.15, page 191.

- Instead of final exam question(s) on “Digital Signature Schemes”, you can solve all of the following:
  - Exercise 12.2, page 484.
  - Exercise 12.8, page 485.

Important Notes

1. The deadline for delivering your answers for the take-home exam is Friday (Tir 4th) midnight. Late delivery by more than 1 hour is not acceptable.

2. All answers must be typeset (use LaTeX or Word + MathType). Handwritten answers are not acceptable.

3. The exam is to be taken individually. Collaboration is not allowed.

4. Your answers should be as formal as possible.