Problem Set 6

We will work on the following exercises together during the work sessions on Tuesday.

The last questions are marked as homework exercises. Your homework must be handed in within one week **electronically via Canvas before Thursday, 14 September 2017, 20:00h**. This deadline is strict and late submissions are graded with a 0. At the end of the course, the lowest of all the homework grades will be dropped.

You are strongly encouraged to work together on the exercises, including the homework. However, after this discussion phase, you have to write down and submit your own individual solution.

Problem 1: Exercise 3.20 from [KL]

Consider a stateful variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is *not* CPA-secure.

Problem 2: Exercise 3.28 from [KL]

Show that the CBC, OFB, and CTR modes of operation do not yield CCA-secure encryption schemes (regardless of F).

Problem 3: Exercise 3.29 from [KL]

Let $\Pi_1 = (\mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\Pi_2 = (\mathsf{Enc}_2, \mathsf{Dec}_2)$ be two encryption schemes for which it is known that at least one is CPA-secure (but you donâĂŹt know which one). Show how to construct an encryption scheme Π that is guaranteed to be CPA-secure as long as at least one of Π_1 or Π_2 is CPA-secure. Provide a full proof of your solution.

Hint: Generate two plaintext messages from the original plaintext so that knowledge of either one reveals nothing about the original plaintext, but knowledge of both enables the original plaintext to be computed.