7. Exercise sheet
Hand in solutions until Friday, 16 December 2016, 12:00 (noon)

Exercise 7.1 (Dilemma). (4+4 points)

Let $\Pi_0$ and $\Pi_1$ be two encryption schemes for which it is known that at least one of them is IND-CPA secure. The problem is that you don’t know which one is CPA-secure and which one may not be. Show how to construct an encryption scheme $\Pi$ that is guaranteed to be IND-CPA-secure.

Provide a full proof of your answer.

Exercise 7.2 (AE). (14+6 points)

Consider the paper


Concentrate on the implication $\text{INT-CTXT} \land \text{IND-CPA} \implies \text{IND-CCA}$, namely Theorem 3.2.

(i) Explain the security notion $\text{INT-CTXT}$. 3

(ii) Choose one of the compositions $E&M$ ($=E&A$), $MtE$ ($=AtE$) and $EtM$ ($=EtA$). Explain how the authors apply their Theorem 3.2 to that composition. 3

(iii) The paper says that IPsec uses a variant of Encrypt-then-MAC. (Mind that due to the date of the paper newer AE modes are not considered here!)

- Find out what is modified. 4
- Do you think it is IND-CCA secure provided the used block cipher is a pseudorandom function? 1
- Argue. 3
- Prove. +6