Cryptography, winter 2015/16

MICHAEL NÜSKEN, SIMON SCHNEIDER

8. Exercise sheet
Hand in solutions until Saturday, 9 January 2016, 12:00

Exercise 8.1 (Dilemma). (4+4 points)

Let Π_0 and Π_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 constuct an encryption scheme Π that is guaranteed to be CPA-secure. $\boxed{4+4}$

Provide a full proof of your answer.

Exercise 8.2 (AE). (14+6 points)

Consider the paper

> Mihir Bellare & Chanathip Namprempre (2000). Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm. URL `https://eprint.iacr.org/2000/025`.

Concentrate on the implication INT-CTXT$\wedge$IND-CPA $\implies$ IND-CCA, namely Theorem 3.2.

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

(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. $\boxed{3}$

(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. $\boxed{4}$
- ○ Do you think it is IND-CCA secure provided the used block cipher is a pseudorandom function? $\boxed{1}$
- ○ Argue. $\boxed{3}$
- ○ Prove. $\boxed{+6}$