Symmetric primitives, winter 2014/15

MICHAEL NÜSKEN

9. Exercise sheet
Hand in solutions until Monday, 12 January 2015, 13:59

Let's have a look at more primitives.

Exercise 9.1 (OTR real-or-random key?). (4 points)

Check whether the key exchange used in OTR provides AKE security. In particular: Is the generated key real-or-random? Prove your answer. 4

Exercise 9.2 (Sign and mac). (8+8 points)

Consider `http://webee.technion.ac.il/~hugo/sigma.html`, in particular the paper given there.

(i) Test your intution. (Figure 1.) 8+2

Which of the four protocols may be a secure authenticated key-exchange? Give a short(!) reasoning in your own words for each case.

Connect the reasoning with the security models discussed for TLS.

(ii) Check the three named security requirements in §2.1 against the security models discussed for TLS. Are they consequences of the TLS security model. +6