Symmetric primitives, winter 2014/15

MICHAEL NÜSKEN

8. Exercise sheet
Hand in solutions until Monday, 15 December 2014, 13:59

Let's have a look at more primitives.

Exercise 8.1 (SSH). (20+4 points)

Consider the newest RFCs considering SSH.

(i) Describe what happens if you connect to a new computer by ssh for the first time. [I guess you have used ssh before, haven't you? Otherwise try it, the computers in the b-it pools may be usable for trying...] 1

(ii) What are the typical use cases? 1

(iii) Describe the SSH protocol architecture. 4

(iv) Which encyrption algorithms are available? For at least two unrelated ones among them specify key and block size. 2

(v) Which MAC algorithms are available? 2

(vi) Describe the key negotiation for mutual authentication. 4

(vii) What do the RFCs say about the following security issues?

- (a) Replay. 2
- (b) Man-in-the-middle. 2
- (c) Forward Secrecy. 2

(viii) Tell me more... +4