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…]

(ii) What are the typical use cases?

(iii) Describe the SSH protocol architecture.

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

(v) Which MAC algorithms are available?

(vi) Describe the key negotiation for mutual authentication.

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

(a) Replay.

(b) Man-in-the-middle.

(c) Forward Secrecy.

(viii) Tell me more…