4. Exercise sheet
Hand in solutions until Monday, 17 November 2014, 13:59

Exercise 4.1 (CRIME or Poodle). (6 points)
Choose either the CRIME or the Poodle attack.
Describe the attack and countermeasures. (Do not forget to properly cite your sources.)

Exercise 4.2 (HMAC documentation). (6 points)
Find the basic, up-to-date RFC for HMAC-SHA1.
Explain how many executions of the compression function are needed, in particular,

- for 55 Bytes. Hint: This should be four.
- for 56 or 57 Bytes. Hint: This should be five.

Exercise 4.3 (TLS documentation). (8+4 points)
Find the basic, up-to-date RFC for TLS and read it.

(i) Under which conditions is perfect forward security provided? Can the client force it? Can the server force it?

(ii) Which endpoint identities does the protocol hide? (Consider three cases: the attacker merely observes, the attacker acts as client, the attacker acts as server.)

(iii) Does the protocol provide live partner reassurance? (Otherwise an attacker can replay possibly modified old messages.)

(iv) Break the newest version of TLS.