6. Exercise sheet

Hand in solutions until Monday, 1 June 2015, 11:59

**Exercise 6.1** (BEAST or Poodle).  
Choose either the BEAST or the Poodle attack.  
Describe the attack and countermeasures. (Do not forget to properly cite your sources.)

**(6 points)**

**Exercise 6.2** (HMAC documentation).  
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.

**(0+6 points)**

**Exercise 6.3** (TLS documentation).  
Find the basic, up-to-date RFC for TLS and read it.

(i) How is the Client’s Finished message composed if the client does not have a certificate?  
(ii) Under which conditions is perfect forward security provided? Can the client force it? Can the server force it?  
(iii) Which endpoint identities does the protocol hide? (Consider three cases: the attacker merely observes, the attacker acts as client, the attacker acts as server.)  
(iv) Does the protocol provide live partner reassurance? (Otherwise an attacker can *replay* possibly modified old messages.)  
(v) Break the newest version of TLS.

**(11+4 points)**
Exercise 6.4 (Capturing TLS).  

(8+2 points)

For this exercise we recommend to use the tool "Wireshark". For privacy reasons, do not include the whole captured pcap files in your assignment (unless you have anonymized them)!

(i) Capture a TLS connection from your computer to the b-it (https://cosec.bit.uni-bonn.de/).

(ii) Answer the following questions for the captured connection.

(a) Which version of the protocol was used? Is it the up to date version?

(b) Which cryptographic schemes were proposed and which were chosen?

(c) Are there identifiers which identify the client? The server?

(d) Describe the key exchange. How many messages were exchanged before the key exchange started? Which key exchange scheme was used? How is it authenticated?

(iii) Do it again with another target with major differences. (Maybe an IMAP connection?)