Exercise Transport Layer Security

Due: 18.10.2010
groups of two students

- choose the library you want – either OpenSSL or GnuTLS
- Install your own CA and release a client and a server certificate
  - submit* all certificates and keys and specify the library you used
- write your own client and server
  - submit* the source code incl all certificates and keys and specify the library you used
- write your own TLS extension
  - submit* the source code incl all certificates and keys and specify the library you used

comments:

A good example for a “How to be a CA” tutorial:
http://www.flatmtn.com/article/setting-openssl-create-certificates – to setup CA
http://www.g-loaded.eu/2005/11/10/be-your-own-ca/ - to issue a server certificate

* send them by mail to latze@iam.unibe.ch