System Administration (LTAT.06.003)

Lab 7
HyperText Transfer Protocol Secure (HTTPS)

- Makes the web secure.
- Uses public/private key cryptography.
- Uses encrypted layer 4 traffic over TCP called TLS (Transport Layer Security).
- Needs the cooperation of the whole world to work due to how Certificate Authorities work.

- Three sides:
  - Server has a private key it will never share.
  - Server has a public key it will give to users, to encrypt traffic to server.
  - Public key is signed against a Certificate Authority, that provides a way to trace the trust layers.

- Exchange of the cryptographic keys is called “Key Exchange”. This is a complicated topic best not explained by us.
HTTPS

HTTP: No Encryption (no SSL)

HTTPS: Secure Cheap SSL Connection
Certificate Authority
TLS lab

- We will try to understand how TLS and HTTPS work.
- Generate our own TLS certificates for our services and set them up:
  - All websites we set up in the Apache lab.
  - Mail services we set up in the Mail lab.
- See if we can connect to them. Check out some wire sniffing techniques.