openssl

openssl is a tool for doing ★SSL aka TLS things★

inspect certificates

create CSRs

sign certificates

It uses the OpenSSL library (or LibreSSL)

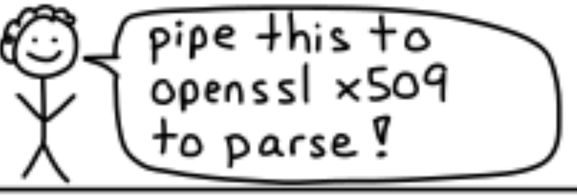
inspect a certificate

```
$ openssl x509 -in
  FILE.crt -noout -text
```

this works for files ending in .crt or .pem! Try it out: you probably have certs in /usr/share/ca-certificates

look at a website's certificate

```
$ openssl s_client
  -showcerts -connect
  google.com:443
```



to get a SSL cert for your website, you need to make a file called a "certificate signing request".

make a CSR

```
$ openssl req -new
  -sha256   -key FILE.key
  -out FILE.csr
```

make one of these with

```
$ openssl genrsa
```

md5 / sha1 / sha256 / sha512

Not quite SSL but useful:

```
$ openssl md5 FILE
```

computes the md5sum of FILE. Same for other digests

```
$ openssl list -digest-commands
```

shows all supported digests.

Introduction

Objectifs du labo

- Protocole TLS: Établissement de clé et certification
- Diffie-Hellman pour l'établissement de clé
  - Attaque de l'homme du milieu
  - Corps finis
  - Courbes elliptiques
- Certification et autorité de confiance