IN3210/4210 Exercise 5 - TLS

(Basic) Apache configuration:

```
<VirtualHost _default_:443>
      ServerName              localhost
      DocumentRoot            /var/www/html

      SSLEngine               on

      SSLCertificateFile      [...]
      SSLCertificateKeyFile   [...]
</VirtualHost>
```

Results of testssl (relevant parts):

```
 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      offered
 TLS 1.1    offered
 TLS 1.2    offered (OK)
 SPDY/NPN   not offered
[...]
 PFS is offered (OK)  ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-
SHA384 DHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA DHE-RSA-CAMELLIA256-SHA
ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256 DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA DHE-RSA-CAMELLIA128-SHA ECDHE-RSA-AES128-SHA
[...]
 Has server cipher order?     nope (NOT ok)
```

Secure Apache configuration:

```
<VirtualHost _default_:443>
      ServerName              localhost
      DocumentRoot            /var/www/html

      SSLEngine               on

      SSLCertificateFile      [...]
      SSLCertificateKeyFile   [...]

      SSLProtocol             all -SSLv3 -TLSv1 -TLSv1.1
      SSLHonorCipherOrder     on
      SSLCipherSuite          ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-
AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-
RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
</VirtualHost>
```

Results of testssl (relevant parts):

```
 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 SPDY/NPN   not offered
[...]
 PFS is offered (OK)  ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-
SHA384 ECDHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-GCM-SHA256
[...]
 Has server cipher order?     yes (OK)
```