## SADS 2019 Problem Sheet #5

**Problem 5.1:** *Pretty Good Privacy (PGP)*                    (2+1 = 3 points)

a) Write down the sum of your matriculation number and  348641573.

b) What is the purpose of a PGP revocation certificate?

**Problem 5.2:** *X.509 Certificates*                         (1+1+1+1+1 = 5 points)

The `openssl` command can be used to create and manipulate X.509 certificates.

a) Write instruction on how to generate a RSA public/private key pair. What key size did you use? Extract the public key into a separate file.

b) Write instruction on how to generate a Certificate Signing Request (CSR) for the RSA public/private key pair created in the previous step. Use the apropriate `openssl` to show the content of the CSR you have generated.

c) In order to sign certificates, you need to setup a Certificate Authority (CA). Explain the process to create a CA. Hint: Take a look at the Debian/Ubuntu Perl script `/usr/lib/ssl/misc/CA.pl` and its `-newca` option.

d) Write instruction on how to sign a CSR with your CA.

e) Create an X.509 certificate and a CA. Get your certificate signed by one of your classmates and help your classmates by signing their X.509 certificates. Upload your certificate to Moodle.

**Problem 5.3:** *Certificate Validation*                      (1+1 = 2 points)

a) Inspect the certificate presented by the web site `https://cnds.jacobs-university.de`. What is the validity period of the certificate? What is the validity of the certificates in the certificate chain?

b) The Online Certificate Status Protocol (OCSP) can be used to test the revocation status of a certificate. In order to make the valication check efficient, TLS servers can use OCSP stapling. Briefly explain how OCSP stapling works.

Do the sites `https://cnds.jacobs-university.de` and `https://beadg.de` support OCSP stapling? Explain how this can be determined.