Information systems security
Cryptographic algorithms (2)

This exercise is a continuation of the previous exercise related to the OpenSSL application and, in addition to symmetric algorithms, asymmetric will be used. It is necessary to answer all the questions asked.
We wil use Kali Linux VM. Start Kali Linux and Linux terminal.

Question: Run `openssl` with the version parameter. Which version of OpenSSL is installed on your computer?
Reply:_____

1. Establishing network connection with OpenSSL

OpenSSL enables the establishment of SSL/TLS network communication with remote servers and monitoring of various connection parameters. The aim of this part of the exercise is to get acquainted with the network connectivity of the OpenSSL package.

OpenSSL can check server bandwidth.
Before running this command, you should check which algorithms the server supports to use one of the supported algorithms with the bandwidth check command.
We'll do that at https://www.ssllabs.com/ssltest/. In Hostname , type student.racunarstvo.hr.
You will use the first supported cipher marked in green (preferred). At the time of writing this exercise it was a cipher: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_ SHA256.
Attention, you will need to modify the result you received on the ssllabs page by removing: TLS_ and WITH_, and to replace the underscore (_) with minus (-). You can also remove _SHA256 or whatever will be the result. Example (above result changed to be compatible with the OpenSSL) -> ECDHE-RSA-CHACHA20-POLY1305
View server bandwidth for student.racunarstvo.hr in 5 seconds with the following command:
`openssl s_time -connect student.racunarstvo.hr:443 –time 5 -cipher ECDHE-RSA-CHACHA20-POLY1305`
DO NOT use copy/paste of the above command – it will probably not work because the minus in the PDF is not the same character as the minus that you need to type. There are more signs that will not be ok, so it is the easiest to rewrite commands not to bother with the problems that copy/paste will produce.
How many communication links have been established? Repeat the test 3 times and write down the data.

_____
_____
_____

Why is the result different with every new run?

_____

Repeat the test for www.google.com. Use preferred cipher for google.com! How many communication links have been established now? Repeat the test 3 times and write down the results.

_____
_____
_____

2. Downloading the certificate

With the folwing command we can download the server certificate:
`openssl s_client -connect student.racunarstvo.hr:443 > racunarstvo.txt`
After about 60 seconds, stop the program (CTRL+C) if the process does not complete on it's own. Edit the file (with nano, pico, vi, gedit or any other editor you know how to work with) and delete everything except text between `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` (do not remove the begin and end lines either). If you want to delete single line in nano editor you can position the cursor on that line and press CTRL+K!
We have received the server certificate in the file `racunarstvo.txt`. Check what's in the certificate with the following command:
`openssl x509 -text -in racunarstvo.txt`

What is the certificate validity (from and to dates)?

_____

For which server names is the certificate valid (X509v3 Subject Alternative Name)?

_____

Which organisation issued the certificate?

_____

Repeat the exercise for www.google.com:

What is the certificate validity (from and to dates)?

_____

For which server names is the certificate valid (X509v3 Subject Alternative Name)?

_____

Which organisation issued the certificate?

_____

Repeat the exercise for ctf.com.hr:

What is the certificate validity (from and to dates)?

_____

For which server names is the certificate valid (X509v3 Subject Alternative Name)?

_____

Which organisation issued the certificate?

_____

3. Establishing the TLS connection

Use the following command to establish the TLS connection (if there is an open port on the firewall – if not, try doing this part of the exercise at home):
`openssl s_client -connect mail.racunarstvo.hr:465`

After the connection was established, type:
`ehlo test`

Which protocol and cyper is used?

_____

What is the maximum email size the server accepts (parameter SIZE)?

_____

Repeat the exercise for mail.petrunic.com

Which protocol and cyper is used?

_____

What is the maximum email size the server accepts (parameter SIZE)?

_____

4. Create and digitally sign the certificate

Certificates are the foundation of PKI architecture. In the business world, certificates are usually signed by the CA. We will start by generating the public/private key pair:

```
openssl genrsa 2048 > host.key
```

Then we will create the certificate using these keys:

```
openssl req -new -x509 -nodes -sha512 -days 365 -key host.key > host.cert
```

Follow the wizard and enter the data you want to (For example, Country HR instead of AU)

View the certificate contents witht the following command:

```
openssl x509 –text –in host.cert
```

What is the certificate validity?

_____

For which servername is the certificate valid (check the CN in the Subject field. If empty – you din't type it ;))?

_____

Which organisation issued the certificate?

_____

Now we will combine the host.cert and host.key in one file:

```
cat host.cert host.key > host.pem
```

That's it. You've generated your own certificate. The problem is, this is so called "self-signed" certifikat trusted by noone, no t even your computer. What is the meaning of that?

_____

_____

_____

Let us create the web server that will use this certificate.
Create test web server with the following command:

```
openssl s_server -cert host.pem –www
```

Test server is sunning on port 4433. Open web browser on your Kali Linux VM and connect to https://localhost:4433

You will see the notification that the web browser doesn't trus the issuing certificate authority. Accept the certificate (ONLY in the exercise. In real life you should NOT accept the untrusted certificates, because someone could attack you with Man in the Midle atacks if you do)

Which protocol and cyppers are used?

_____

Stop the Web server with CTRL+C and start it again. This time use port 443
Which command did you use for that?

_____

Stop the Web server with CTRL+C

5. Create your own CA

Let us create the folders we will use in the process of creating the CA (Certification Authority):

```
mkdir keys
mkdir requests
mkdir certs
```

Create empt files needed fpr this process:

```
touch database.txt
echo 01 > serial.txt
```

Create CA keys. Type the password when asked (Private key should always be protected with the password):

_____

```
openssl genrsa -des3 -out keys/ca.key 2048
```

Create master certificate that will be used to sign other certificates:

```
openssl req -new -x509 -days 1001 -key keys/ca.key -out certs/ca.cer
```

Follow the wizard and anter the data needed.

Generate the certificate request by using the previously generated host.key:

```
openssl req -new -nodes -key host.key -out host.csr
```

Follow the wizard and anter the data needed.

Digitally sign the new certificate request:

```
openssl x509 -req -in host.csr -CA certs/ca.cer -CAkey keys/ca.key -out
signed.crt -days 500 -CAserial serial.txt
```

!!! Parameters ARE case sensitive !!!

Combine the signed.crt and host.key in to one file:

```
cat signed.crt host.key > sigend.pem
```

Test the newly generated certificate by starting the Web server on port 4433 and connecting to it through the Web browser. Who signed the certificate? Check the detailed steps below.

```
openssl s_server -cert signed.pem –www
```

Use the Web browser to connect to https://localhost:443, click on the lock icon in the Firefox browser and click on the arrow right to the computer name you are connected to (localhost). Then click on the **more information**, and **view certificate**
Who signed the certificate?

_____

What is the certificate validity?

_____