1.) Use a web browser of your choice, connect to different HTTPS servers, and collect all TLS relevant information concerning your connections.

2.) Explore the availability of cryptographic implementations in your Java runtime environment. Such implementations are provided by so called *Cryptographic Service Providers (CSP)*. (For more information see: Java Cryptography Architecture (JCA) Reference Guide)
Compile a list of all CSP's and their implemented functionalities.

Hint: Use the method `java.security.Security.getProviders()` to get an array of all instances of type `java.security.Provider` provided by your runtime environment. To get provider specific information, use appropriate methods from the `Provider` class.

3.) Generate some random `int` values in a loop using an instance of the class

`java.security.SecureRandom`.

Measure how long it takes until single calls of the method `nextLong()` return. Use the method `System.nanoTime()` for the measurements.

4.) Calculate the MD5 hash values for the following data:

```
d131dd02c5e6eec4693d9a0698aff95c2fcab58712467eab4004583eb8fb7f89
55ad340609f4b30283e488832571415a085125e8f7cdc99fd91dbdf280373c5b
d8823e3156348f5bae6dacd436c919c6dd53e2b487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080a80d1ec69821bcb6a8839396f9652b6ff72a70
```

```
d131dd02c5e6eec4693d9a0698aff95c2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325f1415a085125e8f7cdc99fd91dbd7280373c5b
d8823e3156348f5bae6dacd436c919c6dd53e23487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080280d1ec69821bcb6a8839396f965ab6ff72a70
```

5.) Download shattered-1.pdf and shattered-2.pdf from https://shattered.io/ and calculate the SHA1 hash values of both files.

Find the minimal and maximal byte positions, where shattered-1.pdf and shattered-2.pdf have different values.

6.) Decrypt the following ciphertext. The corresponding plaintext was encrypted with a single DES encryption in ECB modus with the key `0102030405060708`.

```
8430977b99ef37a939eec6a6a7724f28081052a5562453d494995c4f0324ca4a
0b125004e9428b1aba231184a77ff8c3b0eb36eb1b45963c711455a5eee27cc0
5897d84e8b69abbbc110486300fd2f189a712270f3e185d3d49f3473c8a586f2
e24bbdd123d15afb497557426c1e5209389c76f5792a5384
```

7.) Calculate the HMAC-SHA256 values for the test cases published by NIST's Computer Security Resource Center at:

https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/example-values

8.) Show that the following mappings are bijective and inverse to each other.

$$S_e : \mathbb{F}_2{}^8 \longrightarrow \mathbb{F}_2{}^8, \quad S_e(\mathbf{b}) = \begin{pmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} b_0\\ b_1\\ b_2\\ b_3\\ b_4\\ b_5\\ b_6\\ b_7 \end{pmatrix} + \begin{pmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{pmatrix}$$

$$S_d : \mathbb{F}_2{}^8 \longrightarrow \mathbb{F}_2{}^8, \quad S_d(\mathbf{b}) = \begin{pmatrix} 0&0&1&0&0&1&0&1\\ 1&0&0&1&0&0&1&0\\ 0&1&0&0&1&0&0&1\\ 1&0&1&0&0&1&0&0\\ 0&1&0&1&0&0&1&0\\ 0&0&1&0&1&0&0&1\\ 1&0&0&1&0&1&0&0\\ 0&1&0&0&1&0&1&0 \end{pmatrix} \begin{pmatrix} b_0\\ b_1\\ b_2\\ b_3\\ b_4\\ b_5\\ b_6\\ b_7 \end{pmatrix} + \begin{pmatrix} 1\\0\\1\\0\\0\\0\\0\\0 \end{pmatrix}$$

9.) Identify $\mathbf{b} = (b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7)^\top \in \mathbb{F}_2{}^8$ with integer values in the range from $0 = \texttt{0x00}$ to $255 = \texttt{0xff}$:

$$(b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7)^\top \qquad \longleftrightarrow \qquad \sum_{i=0}^{7} b_i \cdot 2^i$$

Calculate $S_e(\texttt{0xBB})$ and $S_e(\texttt{0x86})$.

10.) Show that there is no $\mathbf{b} \in \mathbb{F}_2{}^8$ with $S_e(\mathbf{b}) = \mathbf{b}$ or $S_e(\mathbf{b}) = \overline{\mathbf{b}}$, where $\overline{\mathbf{b}}$ is the bitwise complement of $\mathbf{b}$.

11.) Prove that $m(x) = x^8 + x^4 + x^3 + x + 1$ is irreducible over $\mathbb{F}_2$.

12.) Let $\mathbb{F}_{2^8} = \{b_7x^7 + ... + b_1x + b_0 \mid b_i \in \mathbb{F}_2\}$ with multiplication defined by reduction modulo the irreducible polynomial:

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

Calculate $(x^5 + x^4 + x^3 + x^2 + 1)^{-1}$ and $(x^7 + x^5 + x^4 + x^3 + x^2 + x)^{-1}$.

13.) Let $\mathbb{F}_{2^8}$ be as above. Calculate $x^8$, $x^{16}$, $x^{32}$, $x^{64}$, $x^{15}$, $x^{51}$ and $x^{85}$.

14.) Let $\mathbb{F}_{2^8}$ be as above. Identify $b_7x^7 + ... + b_1x + b_0 \in \mathbb{F}_{2^8}$ with integer values in the range from $0 = \texttt{0x00}$ to $255 = \texttt{0xff}$:

$$b_7x^7 + ... + b_1x + b_0 \qquad \longleftrightarrow \qquad \sum_{i=0}^{7} b_i \cdot 2^i$$

(i) Calculate the multiplicative inverses of $\texttt{0x3D}$ and $\texttt{0xBE}$. Furthermore, calculate $S_e((\texttt{0x3D})^{-1})$ and $S_e((\texttt{0xBE})^{-1})$.

(ii) Calculate $\begin{pmatrix} \texttt{0x02} & \texttt{0x03} & \texttt{0x01} & \texttt{0x01}\\ \texttt{0x01} & \texttt{0x02} & \texttt{0x03} & \texttt{0x01}\\ \texttt{0x01} & \texttt{0x01} & \texttt{0x02} & \texttt{0x03}\\ \texttt{0x03} & \texttt{0x01} & \texttt{0x01} & \texttt{0x02} \end{pmatrix} \begin{pmatrix} \texttt{0xD4}\\ \texttt{0xBF}\\ \texttt{0x5D}\\ \texttt{0x30} \end{pmatrix}$.

(iii) Prove: $\begin{pmatrix} \texttt{0x02} & \texttt{0x03} & \texttt{0x01} & \texttt{0x01}\\ \texttt{0x01} & \texttt{0x02} & \texttt{0x03} & \texttt{0x01}\\ \texttt{0x01} & \texttt{0x01} & \texttt{0x02} & \texttt{0x03}\\ \texttt{0x03} & \texttt{0x01} & \texttt{0x01} & \texttt{0x02} \end{pmatrix}^{-1} = \begin{pmatrix} \texttt{0x0E} & \texttt{0x0B} & \texttt{0x0D} & \texttt{0x09}\\ \texttt{0x09} & \texttt{0x0E} & \texttt{0x0B} & \texttt{0x0D}\\ \texttt{0x0D} & \texttt{0x09} & \texttt{0x0E} & \texttt{0x0B}\\ \texttt{0x0B} & \texttt{0x0D} & \texttt{0x09} & \texttt{0x0E} \end{pmatrix}$