HTTPS Security using SSL

Back in Chapter 2, we built an unsecure HTTP time server. In this programming challenge we will modify it and build a secure HTTPS time server using OpenSSL.

Acronyms and terms you should know

- HTTPS – Hypertext Transfer Protocol Secure
- TLS – Transport Layer Security
- SSL – Secure Socket Layer
- Authentication
- Encryption, decryption
- Integrity
- Cipher, symmetric and asymmetric ciphers
- Plaintext, ciphertext
- Public key and private key
- Certificates
- SNI – Server Name Indication

Programming Challenge 4

1. For an overview of HTTPS security and encryption, you can either read this comic version https://howhttps.works/ (5 pages all the way to the end) or read the first few sections of Chapter 9, *Loading Secure Web Pages with HTTPS and OpenSSL*, up to and including the section titled *OpenSSL*.

   You should still read the sections in the textbook even if you have read the comic version, or vice versa.

2. Install OpenSSL on a computer following the instructions in Appendix B for Windows, Appendix C for Linux or Appendix D for Mac. You might want to do this on a lab computer if you don't feel comfortable doing it on your own computer. **This is probably the most difficult and time consuming step**. See OpenSSL installation notes below.

3. Read the sections *HTTPS and OpenSSL summary*, *Certificates*, and *Self-signed certificates with OpenSSL* in Chapter 10, *Implementing a Secure Web Server*.

4. Follow the instructions in the section *Self-signed certificates with OpenSSL* to generate your own self-signed certificate.

5. Follow the instructions in the sections *HTTPS server with Open SSL* and *Time server example* in Chapter 10 to create your secure HTTPS time server.

6. Browse to your secure HTTPS time server to make sure that it works.

OpenSSL installation notes

For Windows, **I think** this OpenSSL installation is good.
https://slproweb.com/download/Win64OpenSSL-3_2_1.exe

It is from this site https://slproweb.com/products/Win32OpenSSL.html

After installation, you need to copy the folder **openssl** in

C:\Program Files\OpenSSL-Win64\include\openssl

to the MingW include library directory at

C:\MinGW\include