Homework 2 (Module: Web Security)

a. Prepare a list of common websites (at least 5) which use HTTP protocol and which use HTTPS protocol. Some of the websites can have both options available – identify them.

b. When looking at a web page in a browser, how do we tell if it is HTTP or HTTPS? Clearly specify such signs/symbols for each of the popular browsers, such as Firefox, Chrome, Safari and IE. You may submit screenshots if necessary.
c. Prepare a list of CAs (at least 5) which your personal computer trusts. Browse https://www.cis.ksu.edu/ on your browser. How can you get (from the browser) the name of the CA (say x) which verifies the above website? Now recheck your browser’s list of trusted CAs and see if x is present in the list.

d. During typical mutual authentication between your browser and your bank’s web server, the web server presents a digital certificate signed by a CA, but your browser does not. Why? Then, how does the web server becomes sure that it is communicating with you?