Question Number 8

- Book: Serious Cryptography
- Implement Listing 7-1/7-2 and share the results you get after running 7-2.
- Now replace the compare function in 7-1 with the one defined in Listing 7-3 and rerun 7-1. Share the results.
- You stats should be accompanied by the screen-shots of the actual run.

Solution. In my test environment, typical execution of the program in Listing 7-2 using 7-1 prints execution times of around 0.05002 and 0.04486 seconds, respectively. Whereas, using 7-3 prints execution times of around 0.21990 and 0.19668 seconds, respectively.
As we can see that the differences in output when used 7-1 is large due to which attacker can easily identify the position of the first difference, which is the number of correctly guessed bytes. But that is not the case when 7-3 is used as it used constant time implementations.
Below is the screenshot of the actual run.