Exercise 2

Fredrik Kortetjarvi & Rohullah Khorami

March 3, 2021

Task 1

We have attached in an extra PDF file which is called Task1.pdf

Task 2

Attached in java file by the name of Main.java

Task 3

This function leaks information about passport for example it gives a way different message like wrong mac or wrong challenge. The timing problem is that the execution time is different and it depends on conditions. For example if the mac address fails it gives error message quicker but if the mac address approved and challenge gives an error message it takes longer time.
The solution might be that if we implement an extra condition with a give variable int time $\bar{0}$; and if the Mac or challenge conditions fail we increase the time with one and print out only one error message. In this case the function does not give away any information and it check all condition and the the execution time is the same.

Task 4

Attached in a Junit test in form of PINTest.java

Task 5

Atteched as a pv file by the name of handshake.pv