IoTSSC LAB #6

LAB EXERCISE: BENCHMARKING OF ENCRYPTION PROTOCOLS

OVERVIEW

In this lab you will focus on benchmarking different encryption protocols. The objective is to measure:

1) Code size

2) Memory usage

3) CPU usage/runtime, as different symmetric/asymmetric encryption algorithms and different block/key sizes are employed.

SOFTWARE

You only need the FRDM-K64F board for the following exercises.

You will use the presentation by ARM (provided) and the implementations of various algorithms available here: https://tls.mbed.org/source-code. Note that you do **not** need to download the algorithms from this link.

The TLS library contains the algorithms needed for this lab:

https://github.com/ARMmbed/mbed-os-example-tls Follow the instructions on this page to set up the project.

Each time you navigate into one of the subdirectories (hashing, benchmark etc.) you should run:

mbed deploy to initialize the necessary mbed files.

EXERCISE

Go into the hashing folder and run the example. This will demonstrate a couple of different ways to run SHA-256 hashing.

Can you change this to perform MD5 hashing instead? If not try to figure out why this isn't possible.

Go into the benchmark folder and run the example. This will demonstrate encryption speeds for the algorithms included in the library.

Go into the authcrypt folder and run the example showcasing how to perform encryption. Identify the type of encryption implemented in this example?

Think about how you could incorporate any of functionality demonstrated in this lab into your project. Remember to consider performance trade-offs!