Embedded Systems Security'18

Laboratory assignment 4 (must complete)

weeks of May 8th - May 15th

Having done the basics in JavaCard (getting the process flow up and running) now it's time to do some cryptography. The following two tasks should make you familiar with two JC classes, responsible for hasing and key generation. For now we will be working with `CREF`, and you can leverage examples from the previous list to kick-start your code.

Assignment 1 Write a JavaCard applet which will detect all hash functions available in the `CREF` emulator. Use `javacard.security.MessageDigest` class [1].

Assignment 2 Using `javacard.security.KeyPair` class generate RSA key pair. The applet should return the public key on `INS 0x11` and the private one on `INS 0x22`.

Verify if the keys returned by the applet are in fact RSA keys. Choose some random $m < N$ and encrypt it with the public key e: $\sigma = m^e \bmod N$. Then calculate for the private key $d : m' = \sigma^d \bmod N)$ and verify if $m' \overset{?}{=} m$.

[1] https://docs.oracle.com/javacard/3.0.5/api/javacard/security/MessageDigest.html